

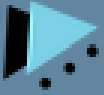
Biometric Platform for your Business

Presented by



In cooperation with the following members





Biometric Platform For your Business

The mindset for security needs to be changed.

Identity is the foundation of Security, without it, governments don't know who to let across their borders, healthcare providers can't recognize their patients, police can't find criminals, corporations can't control access to their facilities and information, and disaster victims and missing persons remain nameless or lost.

Access Verification Solution Limited (AVS) covers many areas regarding biometrics, identity, authentication and access control.

AVS creates a successful and sustainable business proposition through the delivery of convenient and highly secure biometric products and services for all methods of payment and identity protection for various businesses at an affordable price.



Application areas for biometric technologies are constantly expanding, reaching from Government Security, Law Enforcement and Border Controls to commercial, financial and private use.

There are many different areas where biometrics are being used. For example, replacing passwords, protecting against ID theft, account takeovers and multiple accounts as well as screening new customers for on-boarding. e-Commerce sectors include online and mobile banking, payment service providers, insurance, telecoms, retail, health, travel, dating and gambling.

So let us check some interesting articles on the internet and see where AVS can improve the security using the biometric technology available today.

Let us start with the:

NFC Contactless Payment Cards / Contactless payments.

It could have been just another one of those things that happen on the train: a man bumped into a writer for SC Magazine.

Except, as Roi Perez tells it, it all seemed a bit deliberate: the guy slowly bumped into him – and his pocket – for a bit too long.

He said that it took him a minute to realize what had happened.

But when it did dawn on him, he called his bank, only to find out that he'd been e-pickpocketed.

That slow bump had apparently enabled the presumptive thief to get close to Perez's contactless card payment: there'd been an unauthorized £20 snorted from his card to make a transaction on the train.

His bank promptly reimbursed the charge, leaving him to ponder how, technologically speaking, this had happened.

Contactless bank payments usually rely on RFID or on Near Field Communication (NFC) – the same sort of electronics used in public transit cards such as London's Oyster or Sydney's Opal.

(Article Source: <https://nakedsecurity.sophos.com/2015/10/26/train-rider-has-his-contactless-card-e-pickpocketed/>)

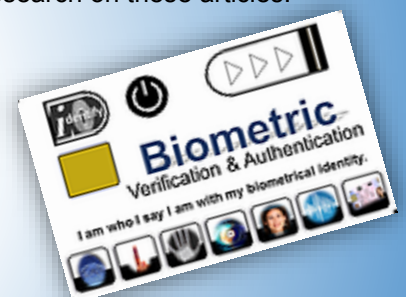
More of these articles

<http://www.ibtimes.co.uk/virtual-pickpockets-steal-money-contactless-bank-cards-by-bumping-into-victims-claims-londoner-1525211> <http://www.dailymail.co.uk/news/article-3451307/The-electronic-pickpocket-Scammer-steals-hundreds-pounds-touching-victims-pockets-sales-device-transferring-cash-contactless-payment-credit-cards.html>

The discussion is, are these articles true? Some people say it's not true and do research on these articles. The discussion and the question should be:

- Why are banks delivering unsecured products?
- Why do banks take the risk and the cost for an unsecured card?

The banks customers are trying to come up with solutions, one of them is to wrap the card in aluminum Foil and make a faraday wallet, why not use the latest technology, a solution could be an on-off button on the credit- or debit card, which can be offered to Banks with our AVS biometric match on card system.



Banking hack heist yields up to \$1 billion worldwide

An international hacking ring has stolen as much as \$1 billion from more than 100 banks in 30 countries in what may be the biggest banking breach ever.

The problem is global and has targeted banks in China, Ukraine, the U.S., India, Sweden and Great Britain. (Article source <http://www.usatoday.com/story/tech/2015/02/15/hackers-steal-billion-in-banking-breach/23464913/>)

The Great Britain (also well known as United Kingdom) financial sector has an increase of loss every year because of card fraud and cyber-attacks.

The body, whose members include banks and credit and debit card issuers, said the figures reflect the "increasing threat" from impersonation and deception frauds, including criminals stealing people's details to commit identity fraud.

A common way that criminals use to dupe someone into handing over their personal details is by cold calling, texting or emailing a victim, claiming to be from a trusted organization, such as a bank, the police, a utility company or a government department.

Often, they will claim that the victim's account needs to be "updated" or "verified" and/or there has been suspicious activity on the victim's account.

Remote banking fraud losses leapt by 72% compared with 2014

Katy Worobec, director of FFA UK, said: "Banks work extremely hard to protect their customers, using highly sophisticated security systems.

(Article source <http://www.dailymail.co.uk/wires/pa/article-3496750/Losses-card-fraud-cyber-attacks-leap-26.html>)



We have seen how hard the banks work on new features, Facial and Fingerprint technology used in banking app's or Selfies using on the mobile devices.

Facial recognition security, even with a "blink test", it's easy to trick.

(article source: <http://www.popsoci.com/its-not-hard-trick-facial-recognition-security>)

Using this feature comes with a big security risk, if your phone is not secure, all your data is potentially at risk. If you ask the experts, they all say, we need more mobile phone security. Unfortunately, not many of us seem to care. Security is a **BIG** issue that is why banks are warning their customers using the technology instead of increasing their security as they claim to do.

Upgrading the Terms of service agreement does not make us more secure.

<http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/11969530/Apple-Pay-warning-Storing-your-partners-fingerprints-is-like-giving-away-your-Pin.html>

Sharing your Touch ID is a big no-no, say banks.

<http://www.cultofmac.com/395626/sharing-your-touch-id-is-a-big-no-no-says-banks/>

If we can use a simple inkjet printer to fool a fingerprint scanner on a mobile device then we need to reconsider our security protocols and use the latest technology to secure our privacy on the mobile devices.

Samsung and Huawei fingerprint scanners can be fooled using an inkjet printer

<https://www.theguardian.com/technology/2016/mar/08/samsung-and-huawei-fingerprint-scanners-can-be-fooled-using-an-inkjet-printer>

Banks don't serve their customers by Not using the latest technology, in our opinion giving an update or a warning just isn't enough.

Biometric technology trials demonstrate a strong willingness by consumers to adopt.

In a recent trial in the Netherlands, 750 bank consumers were enabled for face or fingerprint authentication through biometric identifiers.

Study revealed that 83% thought it was more secure than passwords and 92% thought it was more convenient.

The AVS system secures in a multifactor way the assets from provider and customers.

Banking is essentially about trust. Customers entrust bank with their savings and want to transact securely.

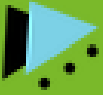
One of the ways to build trust with customers is through innovation like biometric verification.

Biometrics refers to technology that is utilized to verify a person's identity through their biological attributes like fingerprints, voice, iris and facial structures.

Using the latest technology allow us to protect the Provider and the user:

In a World of biometric security, YOU are the password | check out our video here: <https://vimeo.com/169208214>

Biometric spoofing detection | check out our video here: <https://vimeo.com/170445782>



A Samsung spokesperson said: "Samsung takes fingerprint security very serious, and we would like to assure that users' fingerprints are encrypted and securely stored within our devices equipped with fingerprint sensors.

Another thing we see worldwide is the difference in using bankcards.

EMV CHIP DEPLOYMENT STATISTICS



While Europe and Southeast Asia already use the EMV chip card since 2012, a USA Survey finds that six in 10 American credit card holders haven't had their cards replaced.

Fiserv, a provider of financial services technology, estimates that 90% to 95% of retailers aren't ready, while the card was to be implemented on October 1, 2015. General adoption in the USA is planned for 2016 / 2017.

An EMV card is more secure than a magnetic strip card and can help reduce card fraud because the computer chip is embedded in the card.

Video USA is way behind the security for bank cards. <https://vimeo.com/162513536>

More about the EMV chip card

<http://www.usatoday.com/story/money/personalfinance/2015/09/30/chip-credit-card-deadline/73043464/> and here

<http://www.usatoday.com/story/money/columnist/tompor/2015/08/28/new-chip-credit-cards-way-heres-what-consumers-need-know/71337580/>

Still an EMV card needs a signature or Pin code to verify the payment..

Are EMV cards Foolproof?

New Pin and chip hack is revealed by the researchers, where thieves were embedding two chips in a bank card.

While chip & pin (an implementation of the EMV smart card standard) is an improvement on magnetic stripe technology for securing payment card transactions, it's by no means foolproof.

Note that in the US, the industry's EMV implementation is 'Chip & Signature', which is significantly less secure than 'Chip & PIN' (as implemented in Europe and most of the world) because it doesn't take advantage of the PIN authentication feature of EMV?

Retaining instead the written signature, which is relatively easy to fake.

All marketing hype aside, EMV provides greater security for certain types of card transactions (lost/stolen and counterfeit cards), and none at all for others (online, or card-not-present transactions).

And, for the transaction types that it is effective against, we can expect to see more compromises of EMV technology that result in fraud losses as time goes by, until the industry recognizes that it's time to update card transaction security once again.

Lets hope so.... that level of protection is already available to us today.

Access Verification Solutions (AVS) provides a multichannel biometric solution to banking and financial institutions. **AVS assists banks and financial institutions in biometric security in an ever more digital and mobile world through biometric identification and authentication.**

From Know Your Customer (KYC) to online transactions, AVS provides identity verification and authentication solutions.

AVS assists banks and financial institutions to build a multichannel approach, fighting fraud, phishing and identity theft.

Whatever the channel, whatever the service required, whatever the biometric modality selected, Access Verification Solutions proposes a full range of solutions and products to improve customer experiences in a simple and secure way, thanks to biometrics.

Approach Access Verification Solutions biometric technology to build a secure banking and financial environment.

- Biometric as authentication factor
- Access control and security of banks' premises for employees
- Register your customers with Biometrics and manage their real Identity.
- Meets your countries regulatory requirements (even in the USA, some states has other rules and regulations than other States. (Example: under the Illinois law, companies must obtain written consent from customers before collecting their biometric data.) (<http://www.bloomberg.com/news/articles/2016-07-07/do-you-own-your-own-fingerprints>)



Mobile hacks

Another problem when using banking apps is malware.

Millions of customers of Australia's largest banks are the target of a sophisticated Android attack which steals banking details and thwarts two-factor authentication security.

Commonwealth Bank, Westpac, National Australia Bank and ANZ Bank customers are all at risk from the malware which hides on infected devices waiting until users open legitimate banking apps. The malware then superimposes a fake login screen over the top in order to capture usernames and passwords.

The malware is designed to mimic 20 mobile banking apps from:

- Australia,
- New Zealand and
- Turkey,

as well as login screens for:

- PayPal,
- eBay,
- Skype,
- WhatsApp and
- several Google services.

Apart from Australia's Big Four banks it targets a range of other financial institutions including: Bendigo Bank, St. George Bank, Bankwest, ME Bank, ASB Bank, Bank of New Zealand, Kiwibank, Wells Fargo, Halkbank, Yapı Kredi Bank, VakıfBank, Garanti Bank, Akbank, Finansbank, Türkiye İş Bankası and Ziraat Bankası.

Along with stealing login details, the malware can also intercept two-factor authentication codes sent to the phone via SMS — forwarding the code to hackers while hiding it from the owner of the phone.

With access to this information, thieves can bypass a bank's security measures to log into the victims' online banking account from anywhere in the world and transfer funds.

The malware attack has evolved over time, becoming more sophisticated as hackers update the software to defeat security countermeasures.

"This is a significant attack on the banking sector in Australia and New Zealand, and shouldn't be taken lightly," FitzGerald says.

"While 20 banking apps have been targeted so far, there's a high possibility the e-criminals involved will further develop this malware to attack more banking apps in the future."

(Article source <http://www.smh.com.au/technology/consumer-security/malware-hijacks-big-four-australian-banks-apps-steals-twofactor-sms-codes-20160309-gnf528.html>)

Android users who download apps from outside the official Google Play store could be affected by malware targeting Australia's big four banks, explains Fairfax's Tim Biggs.

How this works Tim explains in this video <https://vimeo.com/158880803>

Dozens of malicious Apps on play store can Root and Hack 90% of android devices

It's not at all surprising that the Google Play Store is surrounded by a large number of malicious apps that has the ability to gain users' attention into falling victim for one, but this time, it is even worse than most people realize. <http://thehackernews.com/2016/06/android-hacking-software.html>

Mobile hack becomes more sophisticated, along with stealing login details, the malware can also intercept two-factor authentication codes sent to the phone via SMS — forwarding the code to hackers while hiding it from the owner of the phone.

Biometrics can avoid this problem, also **using the browser instead of the banking app** allow to do more with biometric security.

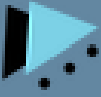
Biometrics seems to be the natural answer to this problem that we have in our hands.

It was a long journey to get to where we act with respect to biometric technology today.

In the modern day, it's the explosive growth of mobile technology that is moving biometric technologies forward, from:

- logging into your phone
- pay with your phone
- mobile wallet
- online banking
- shopping

Governments and companies are all transitioning into biometric security.



Identity and biometrics, it's the natural science of identifying individuals based on their universal unique persistent and convenient features.

We use mobile devices, using these devices from financial to even mobile wallet.

As our mobile devices can be stolen or lost, the critical Question is:

Who's holding the phone,

Use biometrics to secure our mobile devices.

Eye, fingers and voice are features we normally use when we interact with our mobile devices.

We use our computer, laptop and all other mobile devices

How do we identify ourselves today?

We use passwords, but every day we hear about another breach.

Can you imagine 1.2 billion passwords in the hands of one person?

They are not secure anymore.

No wonder because on one hand your passwords need to be:

- Long,
- Complex,
- Different,
- ever-changing

and on the other hand, you should be able to:

- memorize them
- manage them

it's not as simple as it looks.

Biometrics seems to be the natural answer to this problem.

Think about:

- you are not what you memorize
- you are not what you have

Passwords and keys are circuit tokens of identity, you're not them, you are who you are which is biometrics.

Popular Passwords make it easy to hack.

Securing and protecting people's digital identity through biometrics.

Booking a holiday and buying a cup of coffee carry different risks for the bank, retailer and consumer.

AVS secures the provider and the consumers.

We use technology both **visible and invisible** to enable to deliver the best biometrical security available today.

To achieve this, a wider perspective on biometric identity is required.

As leaders in technology, we are developing new solutions around biometric identity.

These enable easier and more secure consumer experiences, while enhancing customer effectiveness and further enabling trust. Ultimately, we want to protect and secure your biometric identity.

As we see of today, a password, SMS verification or pin code is not enough anymore.

Your passwords should be as unique as your fingerprint

Make them less hackable for hackers who use password-guessing software that can run through millions of possible combinations in just minutes.

In addition, if you have an easy password, there may be a hit within 10 seconds.

For many years the words "password", "1234" and "login" are still the most commonly used passwords.

What are people thinking?

Every year, millions of passwords are stolen.

Software can figure out your password, especially when it's on the top 500 list.

(see the full top 500 list through the link below:

<http://www.informationisbeautiful.net/visualizations/top-500-passwords-visualized/>)

These top 500 list is made public by researches, in order of popularity.

Hackers take also advantage of this list.

Using a unique, different and strong password for all of your accounts goes a very long way in protecting yourself from hackers, and that means a different password for every account or site, not just a strong and original one.

A hacker's software will take several years to crack a password like "8guEF\$#gG2#&4H".

Now suppose you have 15 passwords like this (for 15 accounts).

How do you remember them all, being that they're a crazy jumble of all sorts of characters?

Preventing Fraud

Fraudsters will stop at nothing to get your personal information and card data. Their scams can be clever, but not clever enough, if you know how they work and how to avoid them. We've highlighted a few of the ways fraudsters and identity thieves try to get your information.

Phishing:



Phishing is when fraudsters pretending to be from well-known companies, organizations, or government agencies contact consumers and try to trick them into revealing their personal information.

Email Phishing is an email scam that tries to trick you into revealing payment card numbers, Social Security numbers, PIN numbers, bank account passwords or other private information. Most phishing starts as an email that links to a fake Internet site that looks like the real thing with familiar logos and graphics, but is not.

HUNDRED OF PHISHING SITES TAKEN OFFLINE EVERY MONTH

Every month, web hosting companies in the Netherlands receive an average of 470 request from banks to take scam websites offline. The sites are used by criminals angling for confidential details in a practice known as Phishing.

Fewer phishing sites

RTL News obtained the latest figures from the Netherlands Payments Association (*Betaalvereniging Nederland*), which organizes the national payment system for banks, payment institutions and electronic money institutions. The data shows a substantial decline in the number of phishing sites taken offline. Last year, the average was much higher: some 655 such sites per month.

Cost down

The total damage caused by this type of fraud has gone down accordingly. In 2014, total losses stood at € 3.9 million, down from € 4.7 million the year before.

The Netherlands Payments Association puts this down to increased awareness of online dangers on the part of bank account holders. Fewer people fall for fake emails and more people are better able to recognize scam websites.

Biometrics as security on top of a website immediately stops Phishing, you can't send over a finger or your face by an requested e-mail.

Digital Wallet Services Security, Digital wallets can hold personal data, including your payment account numbers, passwords and personal information.

Similar to the way you protect your physical wallet, it's important to protect your digital wallet.

Online, from spyware to shady merchants, the threat of online fraud is real, but you are the best line of defense.

The key to combating online fraud is knowing what threats exist and taking easy steps to beat them.

Retail/ATM, accepted across the world, more convenient and safer than cash, payment cards have transformed how we shop and bank.

Fraudsters may try to steal your card information and use it for unauthorized charges.

Identity Theft, if thieves obtain your driver's license or Social Security number, they can pretend to be you and potentially open bank accounts, order credit cards, write bad checks and obtain loans.

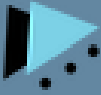
They can also ruin your credit score and make it hard to obtain credit in the future.

Identity thieves use a variety of tactics, even "dumpster diving"

Deceptive Marketing, have you ever signed up for what you thought was a "free trial" then found out months later you've been getting billed for it each month?

Marketers sometimes offer a free trial or free product but may not adequately convey that you needed to "opt-out" before the end of the trial period to avoid a recurring monthly charge.

At Home, Did you know that half of all identity theft is committed by individuals with legitimate access to your home such as live-in caregivers, relatives or renovation crews?

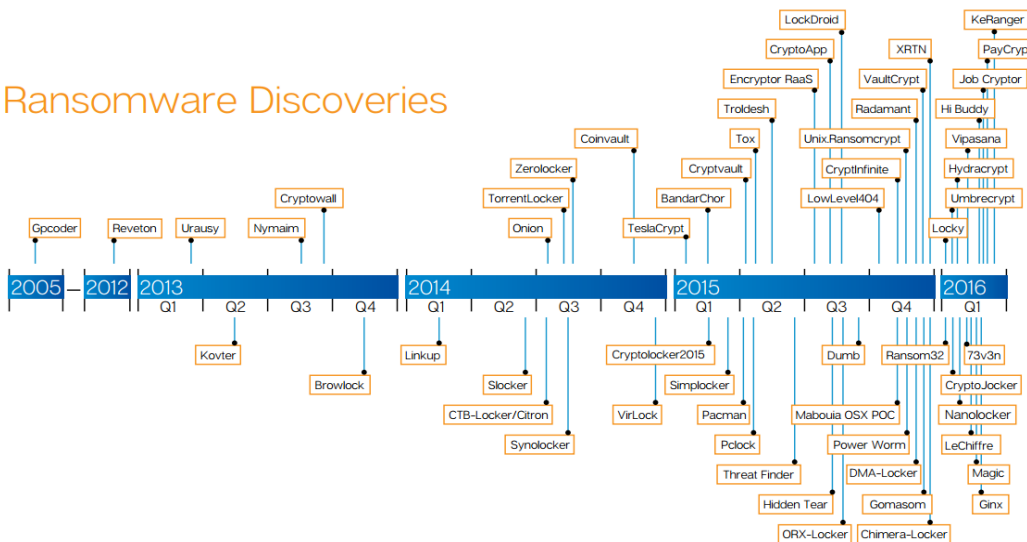


Mail and Phone, fraudsters can send official-looking letters or pose as representatives from Visa, financial institutions or even charities. If asked to provide your account number or other personal information in the mail or by phone, be wary of fraud.

Malware, 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. A very aggressive way of malware, check the latest news here:
<http://www.bbc.com/news/technology-35996408>

Ransomware, is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker)

Ransomware Discoveries



Authentication factors.

Multi-factor authentication is sometimes confused with “strong authentication”. However, “strong authentication” and “multi-factor authentication”, are fundamentally different processes. Soliciting multiple answers to challenge questions can typically be considered strong authentication, but unless the process also retrieves “something the user has” or “something the user is”, it is not considered multi-factor authentication.

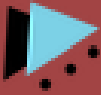
Preventing Fraud, **Multi-factor authentication (MFA)** is a method of multi-faceted access control, which a user can pass by successfully presenting authentication factors from at least two of the three categories:

- Knowledge factors (“only the user knows”),
 - a. such as passwords,
 - b. answers to a specific question.
- Ownership factors (“only the user has”),
 - a. such as ATM cards,
 - b. passport,
 - c. hardware tokens.
- Existing factors (“only the user is”),
 - a. such as biometrics.



The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database.

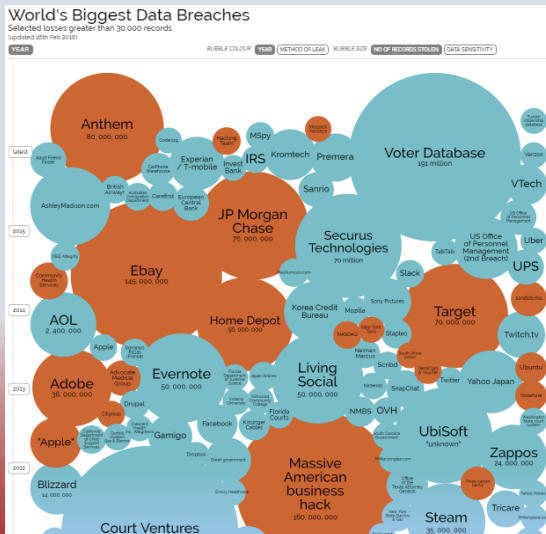
If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.



One of the largest problems with traditional user ID and password login is the need to maintain a password database.

Whether encrypted or not, if the database is captured it provides an attacker with a source to verify his guesses at speeds limited only by his hardware resources.

A password database alone doesn't stand a chance against such methods when it is a real target of interest. In the past, MFA systems typically relied upon two-factor authentication.



Every day we hear about another breach, we can follow them here:

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

We can even sort on what kind of organization;

Academic | banking | energy | financial | gaming | government | healthcare | law firm | media | military | retail | tech | telecoms | transport | web

Or on the method of leak;

Accidentally published | configuration error | hacked | inside job | leak | lost / stolen computer | lost / stolen media | poor security.

It gives us a lot of inside information how the breaches where done, a lot of them could have been prevented if Biometrics had been implemented

One of the hacks in 2016, the IRS Identity Theft Prevention Tool

<https://www.linkedin.com/pulse/irs-identity-theft-prevention-tool-hacked-robert-siciliano-csp?trk=hp-feed-article-title-publish>

Increasingly, vendors are using the label "multi-factor" to describe any authentication scheme that requires more than one identity credential.

A developing world could benefit the most from these new biometric technologies because in the absence of traditional infrastructure such as banking, in places where people don't even have drinking water, but they do have access to cell phones with data connection they can pursue:

- banking financial transactions
- medical transactions and even
- educational services through these mobile technologies

if you think about situations such as:

- natural disasters or
- refugee crises

where biometric could be the only identity solution on hand.

Biometrics, how to do it right?

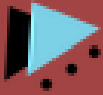
Arguing that the focus should be on privacy and security in the early days of biometric technologies, who's going to control that verified ID, and who has access to it.

Modern biometric technology is user focused and private, so it's changing the old opinions.

It's the user who connects through biometrics for:

- online shopping
- social networks
- online banking
- mobile device

by using their multi-biometrical identity.





Facial web browser solutions.

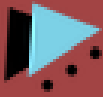
Access Verification Solutions Developed a Facial web browser solution using 2D or 3D facial recognition.

```
/detect/landmarks
{
  "faces": [
    {
      "bottom_right": {
        "x": 565,
        "y": 189
      },
      "landmarks": [
        {
          "x": 504,
          "y": 140
        },
        {
          "x": 503,
          "y": 147
        },
        {
          "x": 503,
          "y": 153
        }
      ]
    }
  ]
}

/recognize/people
{
  "people": [
    {
      "bottom_right": {
        "x": 565,
        "y": 189
      },
      "recognition": {
        "confidence": 0.95,
        "predictedLabel": "Obama"
      },
      "top_left": {
        "x": 493,
        "y": 140
      }
    }
  ]
}
```

These days, many of us regularly feed pieces of ourselves into machines for convenience and security. Our fingerprints unlock our smartphones, and companies are experimenting with more novel biometric markers—voice, heartbeat, grip—as ID for banking and other transactions. However, there are almost no laws in place to control how companies use such information. Nor is it clear what rights people have to protect scans of their retinas or the contours of their face from cataloging by the private sector

IBAN and its members are using the B2B  and B2G  market to roll out their Biometric Solutions. Governments, Banks, Financial institutions and other institutions are able to control your Identity before enrolment of your biometric data, so when it comes to authentication or identification, you can provide that you are you and not another person. Personal enrollment in front of an authority body or related institution who has the permission to ask for your ID is the market for biometric solutions from Qafis and AVS.



e-Passports

An e-Passport contains an electronic chip. The chip holds the same information that is printed on the passport's data page: the holder's name, date of birth, and other biographic information. An e-Passport also contains a biometric identifier. The United States requires that the chip contain a digital photograph of the holder. All e-Passports issued by Visa Waiver Program (VWP) countries and the United States have security features to prevent the unauthorized reading or "skimming" of data stored on the e-Passport chip.

U.S. e-Passport Requirements

The United States requires that travelers entering the United States under the Visa Waiver Program have an e-Passport if their passport was issued on or after October 26, 2006.

Entering the U.S. with an e-Passport

The inspection process for an e-Passport holder is the same as that for a non-e-Passport holder. When arriving at U.S. ports of entry, e-Passport holders will be directed by signage or personnel on the appropriate U.S. Customs and Border Protection both to use.

Benefits of an e-Passport

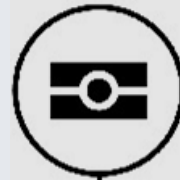
E-Passports help to

- securely identify the traveler,
- provide protection against identity theft,
- protect privacy and
- make it difficult to alter a document for use in gaining admission to the United States.

The biographic and biometric data contained in the electronic chip can be compared to both the traveler and the travel document being presented.

There are multiple layers of security in the e-Passport process that prevent duplication.

e-Passport
symbol



International Cooperation

The United States and its VWP partners have worked together through extensive testing to identify a technology solution to support the production of e-Passports and e-Passport readers. Successful testing in the United States and overseas has been an important step forward in a larger, comprehensive effort to enhance security and facilitate legitimate travel and trade through international cooperation.

<https://www.dhs.gov/e-passports>

How difficult is it to order a fake passport?



Journalist Harald Doornbos managed to get his hands on a genuine Syrian passport displaying a photo of Prime Minister Mark Rutte. All it took was one phone call and a 40 hour wait. "All you need is the telephone number of one of the many passport forgers and converted 750 euros."

Since the outbreak of the Syrian war, thousands of blank passports and the Assad regime's printers have ended up in the hands of Sunni insurgents, according to Revu. These insurgents will sell passports showing any photo given to them to anyone willing to pay.

Doornbos describes the consequences as terrifying as it will be even more difficult for security services to detect terrorist if getting hold of a fake identity is this easy.

Doornbos describes the route a terrorist will take, according to his sources:

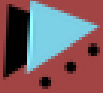
"From an ISIS or al-Qaeda area in northern Syria a returning foreign terrorist fighter will travel to Bodrum in western Turkey. From there he makes the illegal crossing to Greece.

<http://www.nltimes.nl/2015/09/16/journalist-orders-fake-syrian-passport-for-dutch-pm-mark-rutte/>

Another example from a British reporter buy faked #Syria'n ID, passport, driver license for \$2000

<https://twitter.com/markito0171/status/648408334723358720>

If it is easy as we describe above we have a worldwide problem when we want to use a passport or ID card for verification or authentication.



Can things go wrong with a passport?

When applying for a passport things can go wrong, such as:

- Name
- Date of Birth
- Address
- Spelling mistakes
- Wrong or upside down biometric identifiers

The Netherlands (Dutch Article)



Approximately one in ten passports the fingerprints are upside down. This is the result of a sample which was conducted by the National Identity data from the manufacturer of the travel documents, writes Minister Ronald Plasterk (Interior) Friday to parliament. He is exploring whether it's needed to repair it . For several years two fingerprints must be included in a passport. These prints are not visible on the document, because they are incorporated in a chip. Also, when taking the impression, during the processing and regular quality checks by the manufacturer the fingerprint is not visible. Most probably something went wrong by improper use of the equipment with which fingerprints are taken. This is done at the counter of municipalities when someone arranges a new passport. According to Minister Plasterk there are no direct consequences for citizens. The fingerprints are not yet used and it is not clear whether a fingerprint that is upside down, always leads to a "mismatch" at inspection.

(Article source <http://www.telegraaf.nl/e/25373460> translate to English

According to Minister Plasterk there are no direct consequences for citizens. The fingerprints are not yet used and it is not clear whether a fingerprint that is upside down, always leads to a "mismatch" at inspection.

Why collect fingerprints for years and not use them, while we can read about failures in registration and registers. Using of collected fingerprints would have avoid this.

Registration or register Failures

A nice example is the Dutch Bulgarian fraud

A report says the fraudsters register at Rotterdam city council with their ID and a fake rental contract. They are then given an official number (bsn) which they hand over to the fraudsters and then return to Bulgaria. The fraudsters can then use this number to apply for backdated health and housing benefits which can net them €6,000 to €8,000 per person.

The tax office pays out the cash immediately and only checks up on the legitimacy of claims afterwards. In a reaction, junior finance minister Frans Weekers said it is unacceptable the Dutch tax system is being used as a cashpoint machine.

<http://www.bbc.com/news/world-europe-23043543>

<http://www.ft.com/cms/s/0/7afd3bd6-bcac-11e2-b344-00144feab7de.html#axzz45MxkFdix>

Fraudsters take advantage of the different Government systems, because registration systems in different countries are used as cashpoint machine. Its easy money. When Governments don't use all the same registration method this form of threat will always sustain.

Does It mean we can't do anything about it, yes we can, but in 99 percent of the cases we act after the fact, by then it's too late, the damage has been done.

If we want to use our passports or Identity Card for verification or authentication, we need to address the issue of revoking and link ability.

What do we mean by revoking ability?

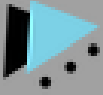
Naive sources of biometrics, like the patterns on your fingerprint or eye patterns, once they're gone, they're gone, you cannot re-issue them.

Their multiple ways to imitate that.

What do we mean by link ability?

We don't want our multi-biometrical identity to be linked back to our data credentials.

Multi-biometrical identity are not only more secure, but they're more accurate.



Storage of Biometrical Data

The data is normally stored on a computer, server, local device, chip or magnetic strip to compare the data of the user.

Unavoidable misuse and abuse of the data information is the reason that Access Verification Solutions Biometric SSL exists.

We believe that biometric identification systems will not create real and serious problems for the honest citizens and will be used on a daily bases.

Criminals want to use biometric Identification systems to their own advantage, to misuse the data and biometric technology.

Criminals can misuse the login details to government databases to create fake passports or apply for government assistance.

This is what we need to avoid!

Hackers stole 5.6 million government fingerprints - more than estimated

(Source Money CNN.com)



Hackers now have a gigantic database of American government employee fingerprints which can be used to positively identify the true identities of those employees.

Hackers stole federal personnel data of 21.5 million people, including federal employees, contractors, and in some cases their friends and family (because of background checks). That includes Social Security numbers and 5.6 million fingerprints.

But cybersecurity experts say the fingerprints could be one of the worst aspects of the theft.

If the hack was indeed committed by foreign government spies, this information isn't likely to end up on the black market for identity thieves.

When identity thieves have access to biometrics and cybersecurity experts announce that obtaining biometric data is the worst aspect of theft, then we need to reconsider our security protocols.

Biometrics are for life, you cannot change your biometrics.

For Access verification Solutions there is a "NO GO" policy when the data from users are stored together with the biometric data without an extra 2-way authentication system.

If we implement biometrics without protecting your identity, we haven't learned anything from the past.

Are Hackers the only threat?

Every company has to deal with Weak Links such as:

- Third-party vendors

Thieves could still find a way to steal data via third-party vendors, which do not face the same level of public scrutiny and do not have budgets to hire cyber security experts of their own and are not as secure as the banks and major retailers or government organizations.

The data breach that hit Target, for example, happened because of a third-party vendor.

- Employees

When Employees Aren't Who They Claim to Be.

There are 7 billion people using thousands of various forms of identification, mostly with little security.

We are functioning in an environment in which humans have yet to be truly verified or authenticated.

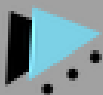
There are thousands of variations of birth certificates, there are people selling fake IDs, from kids on college campuses all the way up to organized criminals; and credit is wide open, which means anyone who gets hold of anyone's identification can get credit under that person's name.

1. Criminals take advantage of the various registration methods:

- a. Databases
- b. File cabinets
- c. Online sales

It's way too easy to pretend to be someone else.

2. In some countries, the Social Security number is related to you, in other countries your birth certificate or even just your name.



Third party Vendor Attacks

More retails hit by NEW third party vendor attacks.

Numerous chains have confirmed that they are investigating potential breaches - some involving payment card data – others may have suffered a hack attack that resulted in the compromise of retailers' customers' names, addresses, phone numbers, email addresses, photo account passwords and credit card information.

Growing Third-Party Breach Concerns

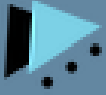
The alert lists a number of security recommendations for managing third-party risks, including using multifactor authentication for remote-access login to point-of-sale systems and including specific policies related to outdated operating systems and software in contracts with vendors.



SWIFT, the global Society for Worldwide Interbank Financial Telecommunications, warned on Thursday of a second malware attack similar to the Bangladesh central bank hack one that led to \$81 million cyber heist.

<http://thehackernews.com/2016/05/swift-bank-hack.html>

SWIFT said in a statement that the attackers clearly exhibited "a deep and sophisticated knowledge of specific operation controls within the targeted banks — knowledge that may have been gained from malicious insiders or cyber attacks, or a combination of both."



Hiring Employees

Make sure you use identity-proofing measures so you aren't scammed.

The first concern most companies have is determining how effective an employee will be.

In fact, the first concern should be determined if the person is actually who he or she claims to be.

Regardless of the nature of your business, an employee masquerading behind a false identity can interfere with your company.

Finally, fake IDs contribute to the disastrous problem of *imposter fraud*.

By reducing fraudulent employment applications, time, money and lawsuits can be avoided.

Eventually, detection methods for fake IDs, such as smartcards, biometrics in all its forms, and multi-factor authentication, will help ensure that the identities presented can be trusted, and being an imposter won't be so easy. Use the AVS Fingerprint smartcard, this smartcard include the latest security technology against lost or stolen smartcards

Ghost workers

Ghost worker fraud has been a chronic problem for many governments across the globe for many years. For most of these countries, billions of tax payer dollars are pumped out annually from the government treasury through salary payments to non-existing employees who have fraudulently been listed in the payroll system.

Some of these employees may include retired civil servants, the deceased or pure fictitious names.

One major reason behind the rise in unqualified, non-eligible individuals is the absence of accountability which allows corrupted civil servants to manipulate government expenditures through the placement of ghost workers on the payroll.

As more governments around the world try to figure out a solution to the ghost worker issue, many are adopting biometrics for identification of employees and time and attendance — a perfect tool for establishing accountability.

How can biometric technology help eliminate ghost workers?

The main advantages of using a biometric system is that it identifies a person by who the person is rather than what the person has, unlike most traditional authorization systems such as personal identification numbers (PINs), passwords, or ID cards. Unlike these solutions that rely on “what you have,” biometric credentials such as a fingerprint, finger vein, palm vein or iris image cannot be lost, forgotten, guessed, or easily cloned.

By utilizing a biometric identification system to eliminate ghost workers, governments and business organization employees can be uniquely identified, virtually eliminating duplicate registration in any form and eradicating ghost worker payroll fraud plus help establish accountability and punctuality among employees. Some of the benefits of using biometric technology include:

Biometric identification eliminates fake employee registration into the payroll system.

If biometric attendance is implemented, the chance of fake time sheets or buddy punching will reduce to nearly 0%.

During salary and benefit distribution, biometric identification ensures accurate disbursement to the right employee.

Biometric identification creates concrete audit trails for employee punctuality which in turn improves service quality.

With ghost workers eliminated, governments and organizations will start generating higher return on investments (ROI).



One of the success stories using biometrics is the **Nigeria Corruption Scandal:**

24,000 Ghost Employees Removed From Government Payroll

The move has allowed the federal government to save about \$11.5 million from its monthly wage bill, according to Reuters.

(Article source: <http://www.ibtimes.com/nigeria-corruption-scandal-24000-ghost-employees-removed-government-payroll-2327092>)

But there are more success stories, as we know from Kenia, Liberia, Malawi and India

All of these successes prove the importance of implementing biometric technology to establish accountability and punctuality.



Conclusion

The problem of ghost workers is that they are often the main source of corruption in many countries. It's not easy to eradicate ghost workers without establishing accountability and a sense of punctuality among employees. Biometric technology can be the perfect tool to establish this and provide a cure to the chronic disease of "ghost worker fraud."

- Know your customers is the latest threat you have to deal with.

Know your customers (KYC) solutions.

Retailers have a legal obligation for age verification before they sell alcohol, tobacco or any age-restricted products to minors. Increasingly, retailers who sell higher value items such as mobile phones and jewelry have an interest in establishing identity to prevent retail fraud.

KNOW YOUR CUSTOMER.



Banks, solicitors and attorneys require customers to provide their identification to prove who they are before financial transactions are made. This is fundamental to the way in which regulated firms manage their fraud risks and comply with their money laundering obligations, such as the Proceeds of Crime Act, PATRIOT Act, and FATF initiatives.

Hotels require identity verification for two main reasons. Firstly, they want to protect against fraudulent credit card use – requiring valid ID at check-in ensures that a room was not booked with a stolen credit card. Secondly, hotels want to protect the safety of other guests – ensuring that only known guests are admitted to rooms.

Casinos and private clubs increasingly need to verify the identities of their clients during enrolment and entry, to verify an individual's age as a protection against illegal, underage activity, and ensure a bona fide clientele.

e-Commerce and e-Business is such a sensitive industry that often requires consumers to identify themselves, biometrics security offers many excellent advantages. Certain forms of identification are easy to counterfeit, which has led to a rise in identity theft today. By making use of biometric technology, the e-industry can enjoy enhanced security, providing consumers with better security which protects their privacy, identity and their internet e-industry like online shopping or paying their monthly invoices.

Trading, Crowdfunding and Payment solution provider websites are vulnerable for hackers.

Where money is involved hackers try to get their hands on, security through AVS-web solution protect the provider and the user.

School's, Access Verification Solution (AVS) has created and developed a system to avoid online fraud for schools.

Using Biometric identification to authenticate students prior to them logging in to the school's internet learning system in an effort to increase academic integrity, detect and prevent loan fraud.

AVS system avoids rising loan and fraud issues for online schools.

AVS ensures that students are who they say they are and eliminate the possibility of login credentials being shared for cheating. (buddy punching)

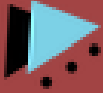
Loan fraud is characterized by fake students dropping classes before the census date, allowing fraudsters to pocket loans with little chance of recovery by schools.

AVS developed biometric identification and multi-factor authentication solution to protect against these threats.

Hackers who create phishing sites are not able to use the biometrics through their website.

AVS set up a Biometric AVS-web solution with a separated biometric server and do not store the data of the provider site.

When hackers hack the data of the provider's site, they can't access the provider's site because the encrypted separated biometric server and the VPN connection we use behind the code sign certificate.



Biometric Safeguarding against criminal and terrorist attack.

Facial and License Plate recognition technology could help prevent the next terrorist attack.

The reality is you are not going to lock down all the public areas in the world, the same way you lock down a boarding area in an airport.

The public would not tolerate or accept it.

In order to avoid an attack, system must have:

- access to a database (Cloud, on Premises, Server)
- system that can recognize (Readers, Camera's, CCTV, etc.)
- a way to alert authorized people (Police, Security on Premises, Guard)

Collecting all three of these at once is the challenge of securing places like an airport departure area or a metro station.

Access Verification Solutions, 2D and 3D facial technology can help in preventing attacks. (Brussels and Istanbul)

Access Verification Solutions facial-recognition contains:

- access to a database that already contains the suspected perpetrators face, (uploaded by authorized people – Intelligence agencies)
- systems that can obtain usable snapshots of people approaching the protected area,
- alert authorized people with a SMS verification on Premises or Police control room.

Facial-recognition-based systems can spot and flag a suspected terrorist and alarm authorized people on the premises, proven technology that has been on the market for several years.

ACCESS VERIFICATION SOLUTIONS

LICENSE PLATE RECOGNITION

Extraction

BD 181 169 BG 251 39
BP7014280 BW2 - 210
DB 311 23 694 Z-4569
SPN106047 M18491 L
0117-398 BN45-217

Recognition

Surveillance setup

5659 GPB

117RTV

Extraction: Uploading license plates into the database.
Recognition: Supports multiple countries license plates and works with parked or vehicles on the move.
Surveillance setup: Comparing license plates to a database, when flagged a alert to authorized people is given.

Access Verification Solutions Plate recognition technology (AVS Plate) can spot and flag a car from a suspected terrorist heading to an airport, crowded subway or public areas.

On condition that the license plate must be present in the database.

Bringing AVS Plate technology out to airports and public area's is like snapping a photo.

AVS Plate works without the needs of a special camera or camera position, support multiple countries license plates and works with parked or vehicles on the move recognition. Different types of setup, including recognition on a local server.

In Brussels, closed-circuit cameras in the airport and the metro clearly did not detect the possible suspects, they captured images that are being used in the investigation, authorities already knew the suspects. Could facial recognition technology in Brussels airport or metro have saved lives?

The attack on Brussels airport does not point to a specific weakness in airport security, the attack happened in a public area.

The question we need to ask ourselves:

- Why aren't we using the technology, which is available today, to prevent us from such attacks?
- Why don't we share info worldwide between all the intelligence agencies?
- It can happen anywhere. How could we prevent it?

ACCESS VERIFICATION SOLUTIONS

FACIAL RECOGNITION

Extraction

Recognition

Surveillance setup

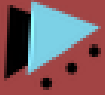
Extraction: Convert a 2D into a 3D image, uploaded into the database.
Recognition: Systems that can obtain usable snapshots of people approaching the protected area.
Surveillance setup: Comparing suspected perpetrators face to a database, when flagged a alert to authorized people is given.

AVS techniques **could help prevent the next terrorist attack**, let's act today and not wait till the next attack to happen.

Biometric technology can help, a facial-recognition-based system must have access to a database that already contains the suspected perpetrator's face, it's up to the intelligence agencies to share pictures to catch a suspected terrorist.

If a suspected terrorist walks into a public area with a facial-recognition-based system, this person is flagged and an alert is given to authorized people.

Image capture technology has improved, not even a whole face is needed, 2D or 3D technology makes this happen.



2D and 3D technology for recognition.

Is the arrested terror suspect the hat-wearing man seen in airport surveillance video moments before one of two deadly terror attacks in Brussels?

That's what investigators are trying to determine after nabbing Mohamed Abrini in a police operation in the Anderlecht district of Brussels.

Technology puts an end to uncertainty about 'man with hat' thanks to special computer program researchers are now 100 percent sure.

(Article source translate to English: <http://www.rtlnieuws.nl/nieuws/buitenland/techniek-maakt-einde-aan-onzekerheid-over-man-met-hoedje>)

Abrini has been tied to the terror attacks on Paris last November through surveillance video and DNA.

Investigators also are trying to determine whether a man arrested in a separate operation Friday was part of the second attack -- at a Brussels metro station -- an hour later. Osama Krayem -- also known as Naim al Hamed -- might be the second person "present at the time of the attack at the Maelbeek subway station,"

(Article source <http://edition.cnn.com/2016/04/08/europe/brussels-attack-arrests/>)

Conclusion

Investigators know the terrorist for a longer time, even their car was known, so basically implementation of facial and license plate registration in and around Brussels Area could have possibly prevent the terroristic attack.

We will never know for sure because the Facial recognition system was not implemented.

Also the way the terrorist escaped from the scene, we know now because cameras could follow them after investigation.

<http://www.usatoday.com/story/news/world/2016/04/07/new-video-might-show-brussels-attackers-escape/82738688/>

One of Brussels airport bombers worked as a cleaner in the EU Parliament

<http://www.newsjs.com/us/brussels-bomber-najim-laachraoui-worked-at-european-parliament-source/dclHPE5V6IV0J5MaUNOTrU3jxkdoM/>

Other biometric technology can also be used in areas like airports.

Fingerprint identification or Iris scans can provide a useful identifier and are becoming easier to collect.

Most people are already using a passport or ID-card that includes biometrics features.

We only need to ask ourselves, how are my biometrics being stored, can it be hacked.

Access Verification Solutions Biometric Secure Socket Layer (AVS BSSL) techniques does not store real images from biometric features.

AVS biometric systems make it far more possible for industry to adopt all biometrics, one integration in one platform, the consumer wants biometrics, they see it's easy to use.

AVS specifically addresses privacy concerns by never storing a person's biometric feature.

AVS creates a unique HASH that have no value and is useless for hackers.

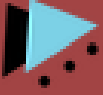
The biometric hash is stored in a separated database from users' credentials.

Biometric solution offers greater security.

ACCESS VERIFICATION SOLUTIONS HAS CREATED AN INNOVATIVE BIOMETRIC PROGRAM IN AIRPORT SECURITY FOR PASSENGERS AND NON-PASSENGERS. THE AVS-CARD (ACCESS VERIFICATION SOLUTION BIOMETRIC SMART CARD) AUTHENTICATION SYSTEM IS INTEGRATED INTO A SMALL CHIP, A PROCESSOR AND A MEMORY IN WHICH TO STORE ENCRYPTED TEMPLATES OF THE FACE AND FINGERPRINTS.

IN ADDITION TO THE AVS-CARD, AIRPORT AUTHORITIES ARE ALSO USING IRIS, FINGERPRINT AND PALM READERS, AS WELL AS A NETWORK TO CONNECT A CENTRAL BIOMETRIC DATABASE WITH SEVERAL OTHER AIRPORTS. ACCESS VERIFICATION SOLUTIONS TAKES AIRPORT SECURITY VERY SERIOUSLY.

With thousands of passengers flying domestically and internationally coupled with the hundreds that cross our borders every day, it is paramount that our airports and border security have the best identification systems in place to reduce the threat of terrorism and control illegal entries into the country.



Integrated Biometrics patented Biometric System on card is ISO/IEC certified and provides the ideal solution to protect our nation's borders. Biometric identification systems are fast becoming a standard within National border control Centre. e-Gates has found a path in many airports. AVS-card solutions allow border control officers to provide both security and convenience to its passengers. The solution for secure access, thanks to biometric technology integrated into Smart Cards or passport.



National Identification Applications

- Passport,
- ID card,
- Driving License (i.e. taxi license),
- Healthcare card

AVS-card solutions, a smart card through which physical and logical access will have an unthinkable level of security.

Border controls strike the balance between security to confidential information and excellent, convenient customer service.

An easy system for the user, using the existing infrastructure they already have implemented.

AVS-face solutions allows airports to use the mobile application.

AVS-face solution is a 3D empowered mobile app solution designed for online check in industries.

Using the Biometric-matching server for verification and Authentication designed to protect the safety of the end users, a step ahead in safeguarding against criminal and terrorist activity.

Using Biometrics to safeguard identities.

The use of biometrics provides an accurate way to verify identities using unique physiological characteristics, such as fingerprints, iris and facial features.

In accordance with local country Policy on Biometrics and Refugee Registration and Verification, biometrics should be used as a routine part of identity solution to ensure those refugees' personal identities cannot be lost, **registered multiple times** or subject to fraud or identity theft.



ISIS ATTACKER LIVED IN GERMAN REFUGEE SHELTER, CLAIMED TO BE SYRIAN

The man was known to German authorities under at least seven different identities before, committed numerous offenses and was serving a one-month prison sentence in August, the director of the bureau of criminality North Rhine-Westphalia, Uwe Jacob, said

<http://www.frontpagemag.com/point/261410/isis-attacker-lived-german-refugee-shelter-claimed-daniel-greenfield>

Healthcare. Securing Electronic Health Data

There is no doubt that biometrics has significant potential in:

- health care,
- facilitating cost reductions,
- enhancing information security,
- improving accessibility and
- increasing service quality.

Securing electronic health data, in scenarios in which the provision of care services is shared among multiple actors, could become a complex and costly activity.

Correct identification of patients and physicians, protection of privacy and confidentiality, assignment of access permissions for healthcare providers and resolutions of conflicts rise as main points of concern in the development of interconnected health information networks. Biometric technologies have been proposed as a possible technological solution for these issues due to its ability to provide a mechanism for unique verification of an individual identity.

The most effective solution to prevent fraud and medical identity theft in healthcare is to strengthen the authentication and minimize the risks of security breaches with the use of biometrics. (biometric healthcare smartcard)

Biometrics has been becoming the best choice for the healthcare provider to solve fraudulent issues. In recent years, biometrics has been adopted by various healthcare organizations worldwide to protect health records, facilitate easier access to medical information, and defend health care consumers against fraud.

Besides, the rise of multi operable health information databases using biometrics can enable services to simply and regularly administrate the access to medical identity by authorizing access to patient's records using biometrics.

By linking such information, the patients can be easily identified and connected with their personal medical records providing for specific healthcare services.

Hence, the link between biometrics and electronic health records allows the health organizations to provide more accurate and efficient healthcare services.

Governments around the world requires that physicians and healthcare professionals who use electronic health records should carefully check the access to the patient's record.

Biometrics allows the physicians and professionals to do this easily.

AVS Health patients-access makes the records only accessible to someone who is identified by our multi-approach biometric technology.



A biometric Smartcard helps to:

- secure patient data,
- de-duplicate data and
- patient identification.

The data is only accessible when the owner has given permission to see these personal files.



AVS can ensure that the person who accessed the file is definitely the one that has the right to see the patient's data.
If they mismatch, the appropriate authorities can be notified that an unauthorized person is trying to access secure data.

Healthcare biometric market has envisioned a tremendous growth in the past few years.

According to 'Healthcare biometrics market' report, the fingerprint recognition technology is the most prominently used biometric technology and will make up more than 50% percent of biometrics demand in healthcare industry through 2019.



Face and iris recognition are also expected to have rapid growth in terms of the demand for logical access control in healthcare services. AVS can combine the Physical and Logical access control from multi Biometrics together. 1 implementation, 1 platform, all Biometrics.

To push biometric technology into the mainstream identification market, it is important to encourage its evaluation in realistic contexts and foster innovation of inexpensive and user-friendly implementations.

It's bad enough to get hit by a cyber-attack. Don't let a lawsuit hit you too.

For company executives, data breaches are traumatic.

They must rush to patch data leaks and work with law enforcement while also reassuring anxious customers and employee about fraud and identity theft.

And then there's the lawsuits.

After cyber criminals strike, class action lawyers are rarely far behind.

In the wake of breaches at retailers like Home Depot, Michaels and Target, lawyers have been quick to pounce by filing complaints seeking millions of dollars in the name of consumers.

The outcome of such cases has been mixed, but the good news for executives is they can take steps before and after a breach to minimize exposure to civil lawsuits.

\$7.5M Healthcare Data Breach Settlement

DATA SECURITY MUST BE A KEY FOCUS IN ANY ORGANIZATION IN ORDER TO MITIGATE RISK

In what as being described the "largest per-person data breach settlement on record," a California court approved a \$7.5 million settlement in a class-action lawsuit relating to a breaches of health information in 2011 and 2012.

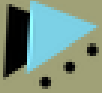
The plaintiffs had brought four causes of action:

- Violation of California's Confidentiality of Medical Information Act
- Negligence
- Money had and received
- Violation of the California Unfair Competition Law

Since this breach in 2012, attacks on patient health data have generally grown "increasingly sophisticated" and are becoming more targeted.

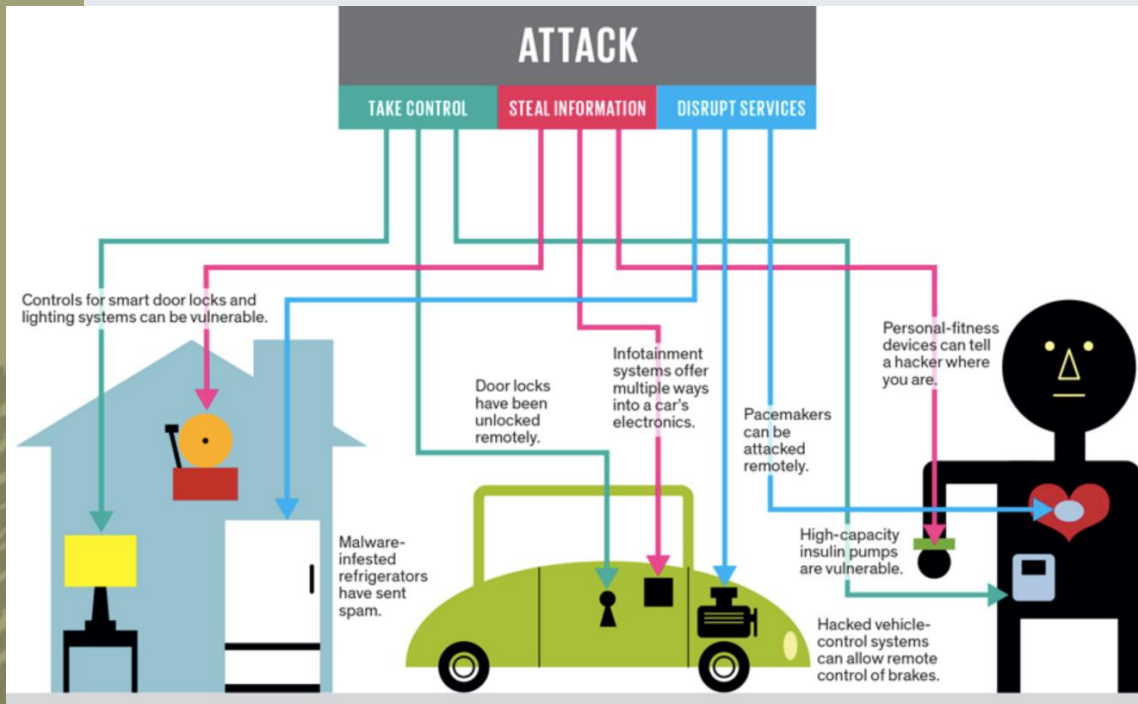
(Article source <https://casetext.com/posts/75m-healthcare-data-breach-settlement>)

As in football, the saying "the best defense is a good offense" is applicable to data security. Actively taking precautions against data breaches is the best -- and only -- way to mitigate risk and to avoid the numerous negative consequences that occur after a data breach.



Therefore, you really want to make sure that:

- the car that you're driving knows it's you who's trying to control it not a hacker.
- The smart door knows you are open the door and not a thief.
- The fridge not sent spam or sent malware to your wifi router
- The personal fitness device can tell a hacker where you are.
- The pacemaker can be affected remotely.
- The insulin pump can be stopped by hackers



Cell phones and tablets are the most common devices we carry to verify or biometrically identify, these devices interact directly with their surroundings and our physical world.

A recent study from Binghamton University also suggests your smartwatch or fitness tracker is not as secure as you think – and it could be used to steal your ATM PIN code.



Retrieving Passwords and PINs Using this Algorithm

Researchers say their "Backward PIN-Sequence Inference" algorithm can be used to capture anything a person type on any keyboard – from automatic teller machine or ATM keypads to mobile keypads – through infected smartwatches, even if the person makes the slight hand movements while entering PINs.

Read the full story here:

<http://thehackernews.com/2016/07/hacking-smartwatch-atm.html>

Biometrics are the natural answer to an identification process that is using biometrical identifiers, something only the user knows, has or is.

Imagine a future where our digital lives are secured, your privacy is preserved and even countless lives are saved. When doors refuse to operate for unrecognized users in restricted areas on airports, buildings or nuclear plants, not excepting unauthorized people to access.

When computers can't operate because the biometric identity were fake.

The Internet of things or connected devices are the next big concerns, as more Internet connectivity means more access points which mean more opportunities for hackers. When it comes to the threat to Internet of Things, Car Hacking is a hot topic.



Since many automobiles companies are offering cars that run mostly on the drive-by-wire system, a majority of functions are electronically controlled, like instrument cluster, steering, brakes, and accelerator.

No doubt these auto-control systems in vehicles improve your driving experience, but at the same time increase the risk of getting hacked.

Recently, security researcher Benjamin Kunz Mejri have disclosed zero-day vulnerabilities that reside the official BMW web domain and ConnectedDrive portal and the worst part: the vulnerabilities remain unpatched and open for hackers.

Biometric Security Solutions.

The primary value proposition of using biometrics over traditional security (in the case of access control) is that it dramatically enhances security by providing multi-factor biometric authentication: your fingerprint, face, eye, palm, vein, voice or biometric smart card.

The days of using a PIN for multi-factor are gone since PINs can be passed on from employee to anyone.

The vast majority of electronic access control systems in place today authenticate the badge, not the person holding the badge.



Where is the security in that?

Solutions such as a biometric Smart card allow implementation of multi-factor authentication without replacing a single reader.

AVS Biometric Smartcard products improves security, there is no data of the employee stored on the separated Biometric database.

AVS specifically addresses privacy concerns by never storing a person's biometric feature. AVS creates a unique HASH that, by themselves, have no value and is useless for hackers. Taking the same amount of time to use a biometric product as a traditional PIN-based card is a biometric solution that offers greater security.



1 Integration, 1 Platform, Any form of Biometrics

Using AVS "Omni" Biometric Platform gives your organization the freedom to work with all biometric technology available today.

Our customized interface software integrate all forms of Biometrics.

The AVS-biometric SSL secures all biometric technology.

Why Limit Your Success with a Biometric SDK?

Many biometric hardware manufacturers offer an SDK, but it ONLY works with their devices.

That means if you develop your biometric matching software using their biometric SDK, you are forever locked into using their devices.

In addition, you are forever locked into a single form of biometric recognition!

If it does not work reliably for all users, or you experience challenges with their biometric hardware, your success rate is greatly limited.

Why Limit your security with a local stored biometric solution.

AVS "Omni" Biometric Platform Provides Flexibility, using all available biometric technology.

Access Verification Solutions interface enables you to tailor your deployment model based on the unique needs of your customers and/or end users, and easily switch between four biometric engines without having to install any new software.

This unparalleled flexibility produces near 100% read rates for any user, under any condition, and results in the lowest possible total cost of ownership compared to other options.

With AVS "Omni" Biometric Platform, never get locked into a single form of biometrics or a single biometric reader.



We have integrated a multifaceted approach to our security to make sure that multiple measures are in place to ensure the security.

The "Omni" channel network secures the separated stored biometric data and matches with the stored encrypted biometric data.

When thieves can change biometric data on a local device or card, we know that this is the worst aspect of theft.

That is why Access Verification Solutions and Qafis have developed the biometric SSL match server.

When the biometric data is replaced on a stolen or lost device or AVS-card, the biometric match server will reject the thief if he tries to access.



Automated Fingerprint Identification System (AFIS)

The **Automated Fingerprint Identification System** (AFIS) is a biometric identification (ID) methodology that uses digital imaging technology to obtain, store, and analyze fingerprint data. The database contains the Biometric features, collected during the biometric enrollment process.

Automated Biometric Identification System (ABIS)

The **Automated Biometric Identification System** (ABIS) provides a real-time biometric identification. *Multi biometric capacity:* processes fingerprints, recognizes faces and allows all other biometrics such as Iris, Palm and Voice.

Accuracy: Integrates biometric engine which provides the latest level of algorithm accuracy, so that customers benefit from the most recent improvements in research & technology.

Efficiency: customized solution, is given the choice between different verification processes depending on the type of use, adjusting what is handled automatically by the ABIS

Interoperability: seamless connectivity with third party systems (other ABIS systems, booking stations or mobile terminals) Compliance with international standards set by: ANSI/NIST and other international standards.

Verifying Identity through Biometrics



Set up a Secured Biometric Database (BSSL)
The Provider Database communicates with the Biometric Database through the VPN connection.
Discover the Biometric Solution for payments and secured access.

Biocryptographic Secure Socket Layer (BSSL)

A significant global growth of the fingerprints or other biometric security solutions by users for authentication is used latterly in a growing way and this made the biometric security a well-known technology.

Consequently, this will increase the application of biometric security features such as fingerprint readers, voice authentication mechanisms as well as facial recognition systems in social networks for a stronger security.

In the near future, Biometric security will be a standard feature in smartphones, but also in other mobile devices.

Biometrics in the future

Biometric solutions are widely used, essentially in smartphones.

These mobile devices contain a massive amount of sensitive personal information, such as private correspondence or medical records as well as timetables and business information.

In the case of a stolen device, the user will never know if a thief uses the device to gather information from the device.

In the case of a lost phone, you never know what the finder does with it.

Biometric solutions protect devices from strangers' access, using different authentication, automated methods like a fingerprint, voice or iris scanning as the highest security level.

On the other part, diverse medical organizations offer services of collecting and employing biometric patients' data.

In addition, the use of the biometric solutions became larger in the cloud.

Therefore, all this biometric data is sensitive information that requests different pertinent solutions from developers to be adequately registered, stored, secured, optimized, shared and administered.

Both digital biometric records and storage need significant security planning to protect the servers storing sensitive biometric data of hacking, as well as to prevent damaging consequences for individuals which own personal physical characteristics on these servers.



Why do we store Data and Biometric features together?

Access Verification Solution offers a separated Biometric database.

AVS doesn't store data from providers users, but makes a connection through VPN behind a Code sign Certificate.

The BSSL (Biometric Secure Socket Layer) solution is more secure.

BSSL aims to enhance the aforementioned security and usability problems by integrating biocryptographic authentication capabilities with the SSL/TLS handshake protocol in a usable, secure, privacy-preserving manner.

Our explanation shows that the BSSL handshake protocol is usable and practical in terms of the time required to complete the handshake protocol by comparing to TLS v1.2 handshake protocol.

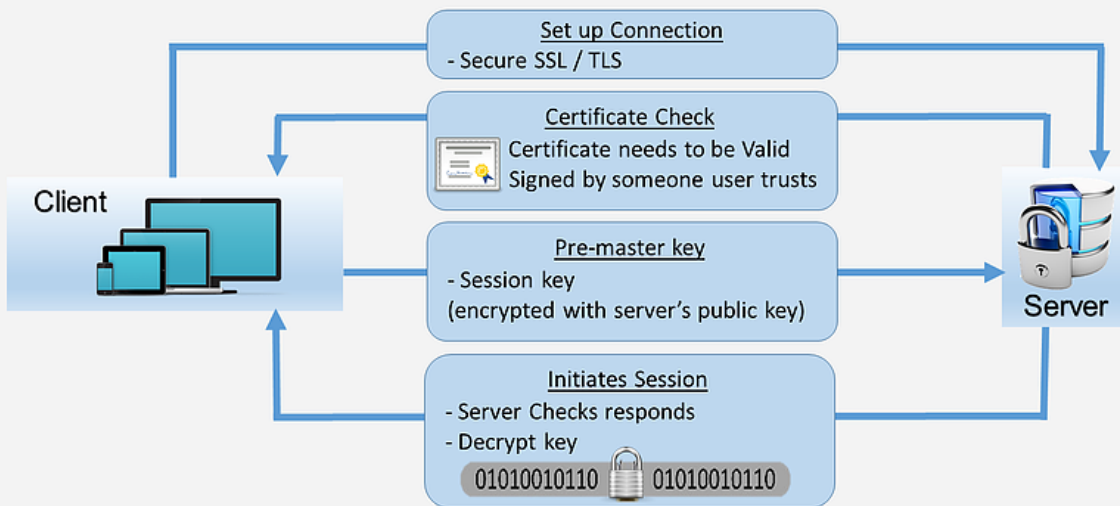
BSSL certificates are used to encrypt the transmitted biometric data, between the data server and the biometric server or from a mobile device to medical organizations as well as vice versa, or between cloud and local databases to end-users devices.

Access Verification Solution provides BSSL certificates that contribute to end-users' private information insurance and confidence.

Explanation between SSL/TLS and BSSL structure:

Explanation between SSL/TLS and BSSL

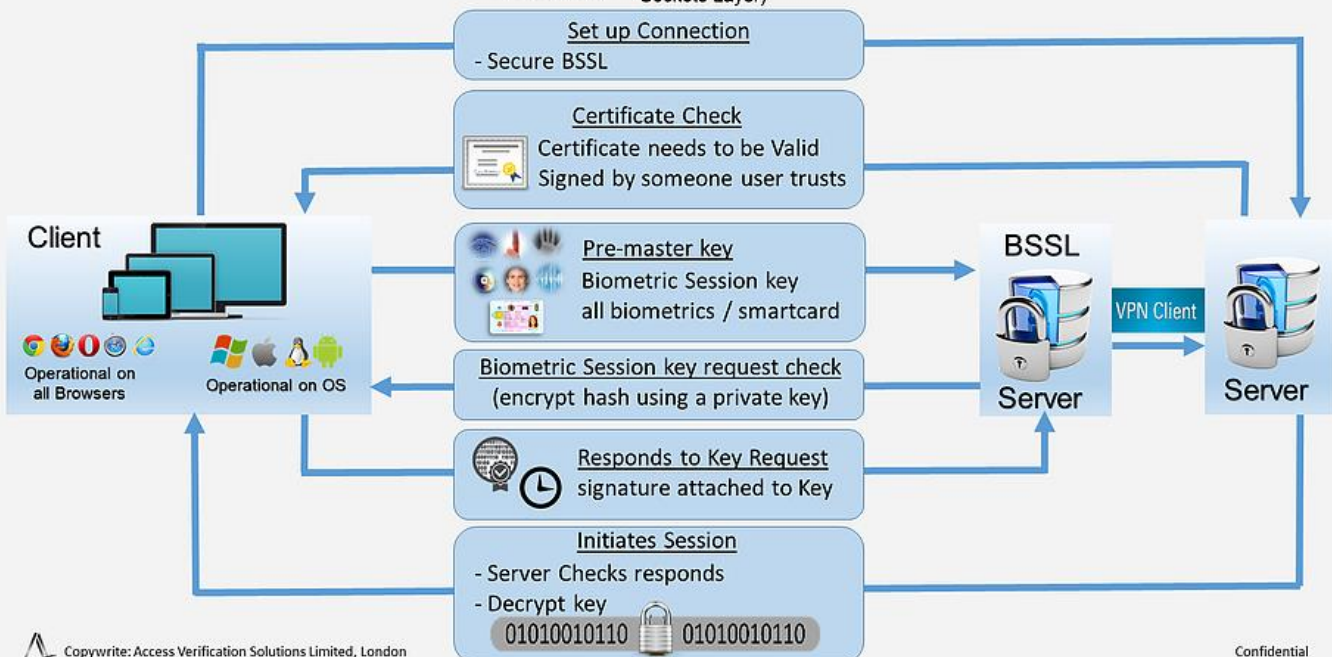
SSL (Secure Sockets Layer) / TLS (Transport Layer Security)



Copyright: Access Verification Solutions Limited, London

Confidential

BSSL (Biometrical Secure Sockets Layer)



Copyright: Access Verification Solutions Limited, London

Confidential



Biometric system on Card. It makes the difference. Data security, authentication, confidentiality.

Innovation with current standards.

Access Verification Solutions has created an innovative biometric program for Governments. The AVS-card (Access Verification Solution Biometric Smart card) authentication system is integrated into a small chip, a processor and a memory in which to store encrypted templates of the face and fingerprints.

Biometric technology offers advanced verification for employees in every industry. Because biometric systems identify people through physical measurements of unique human characteristics or behavior, they thwart attempts of time fraud, where one employee punches in for another. Biometric systems do not require easily lost or stolen badges, or other identifying objects. Employee attendance verification is a major use of biometrics today.

The AVS-card will be used to ensure that the individual to whom the card was issued is the individual who is actually showing the card at the access point, door or computer. Additionally, the AVS-card can be used to verify if the individual who was issued the card still has an active security clearance and if the card is still valid. Stolen or lost cards are easy to deactivate. When a card is stolen and fingers are replaced to gain access they will be rejected by the system. Replacements of biometrics on the stolen card will not match with the "old" biometrics. The Biometric SSL technology authentication system rejects the access.

A big advantage for Access control in buildings where you definitely don't want to have unauthorized people. (Think about Nuclear power plants, Prison, Flight towers, Government Parliament's, Hospitals, Pharmacy, Armored car, etc)

Is Biometric Employee Verification Right for your Organization?
Several factors can help you determine whether to invest in biometric time recorders.
Evaluate the need for authentication or identification.
Consider the cost/benefit ratio.
Assess the compatibility of the biometric technology with the work environment.
Be sensitive to the concerns of employees.

Let AVS or Qafis help you to choose the best Biometric solution for your organization, contact us.



The possibilities of biometrics for employee verification or authentication are endless. Experts attest that biometric technology is likely to be used in "almost every transaction needing authentication of personal identity."

Biometrics are easy to use, it increases our corporate security and improves employee privacy.

As part of our integration process, we work with your company to meet every requirement with our customized technology.

The system is developed to work with a variety of biometric devices, the software is specifically designed to be integrated into existing platforms or access control systems.

Biometric SSL is an affordable solution.
A custom made quote will be made upon request.



Unfortunately it usually takes an incident to force the realization security is a must, it's actually an investment in safety.

Safety of your data, your money, and most importantly your reputation.

We need less vulnerabilities and Stronger Encryption

LIST OF CYBERSECURITY TECH AREAS, PRIORITIES AND EMERGING TRENDS

Emerging Technology Areas:

- Internet of Things
- Wearable's
- Drones and robots
- Artificial intelligence
- Smart cities
- Connected transportation
- Quantum computing

Priorities:

- Protecting critical infrastructure through technologies and Public/Private cooperation
- **Better encryption and biometrics (quantum encryption, keyless authentication)**
- Automated network-security correcting systems (self-encrypting drives)
- Technologies for "real-time" horizon scanning and monitoring of networks
- Diagnostics and forensics (network traffic analysis, payload analysis and endpoint behavior analysis)
- Advanced defense for framework layers (network, payload, endpoint, firewalls and antivirus)
- Mobility and BYOD security
- Big data
- Predictive analytics
- Interoperability

Trends:

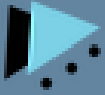
- Informed risk management
- Emergence of public/private sector partnerships
- More information sharing and collaboration between the public and private sectors
- Shared R & D spending
- Increased spending for cloud computing
- Consolidation of data centers
- Expansion of hiring and training of cybersecurity workforce
- Tech foraging

Access Verification Solutions:

- The Changing Face of Security
- Let's create a secure environment with Biometrics

Qafis Biometrics:

- Let the biometric security technology work for you
- I am who I say I am with my Biometrically identity
- A step ahead in biometric solutions



In a world of
biometric
security,
YOU are the
password.



In an era of increased privacy concerns and data breaches, Qafis is building a stealth solution to keep our biometric data safe.

"We see all tech giants claiming they have the safest and stealthiest systems but it's those same companies being the target of major data breaches and discovered vulnerabilities in their systems after years of use"

Edwin Nicolaas, CEO of Qafis

Notable recent breaches in the tech scene include LinkedIn and Adobe but the fintech sector is not immune to this either. Think about the recent Swift banking network hack, which affects banks worldwide. One other major hack last year, 5.6 million fingerprints were stolen from the US government employee database. "A major issue is that many applications and institutions still store privacy data and biometrical data together and locally", says Edwin. Whether you would like to use biometrics to improve your customers' relationship, or to secure daily operations for accessing services, Qafis can provide the technology where security, reliability, accuracy and speed are the solution to build a trusted environment through biometrics.

The BSSL (biometric Secure Socket Layer) solution creates a layered defense and makes it more difficult for an unauthorized person to access a target such as a physical location, device, network, application or database. Qafis has a system that uses biometric characteristics to authenticate identity for secured access.

The BSSL solution is more secure and accurate, because the biometric data is never stored as a template, Qafis creates an encrypted stored and anonymized biometric database which cannot be linked back to the data credentials, making the biometrical data (a hash) useless in case of a breach. Would a bank or government using Qafis' system get hacked then customer biometrics would still be safe on another server. Of vital importance, according to Edwin, as biometrics is something you cannot change as is done with passwords.

The Qafis system has endless applicability's where increased security is needed, for example banking, government and healthcare. Also the new internet of things market is one of Qafis targets. As more and more devices are connected to the internet, the more we are prone to cyber attacks. While someone hacking into your internet connected fridge could only do minor damage, it becomes more risky if hackers target internet connected cars or power generators.

Currently Qafis is running a few pilots. In one of those, they use their solution to increase airport security by adding an extra biometric identification layer to ID cards used by personnel to access restricted areas. With this new addition, called a biometric smartcard, access can only be granted to areas when the ID card matches with the biometric information on card and the separated biometric server. When a card is stolen and fingers are replaced, the Biometric SSL technology authentication system rejects the access.

Replacements of biometrics on the stolen card will not match with the biometric server. A big advantage for Access control in buildings, to prevent unauthorized people. (This technology can also be used in Nuclear power plants, Prisons, Flight towers, Government Parliament's, Hospitals, Pharmacy, Armored car, etc.)

This is just one of the many fields in which the Qafis solution can increase security. In the coming years [Qafis](#) wants to run more pilots in its main areas of interest, as Edwin puts it: "we have a solution for everyone, use biometrics as security for a safer environment, preventing Identity theft, phishing and fraud".



IBAN

**International Biometric
Advisory Network**

223 Regent Street,
London,
United Kingdom,
W1B 2QD

Phone: +44 20 32 89 89 55

<http://www.iban.solutions>



Email | support@access-vs.com
WWW | <http://www.access-vs.com>
Phone | +31 303 200 001



Email | support@qafis.com
WWW | <http://www.qafis.com>
Phone | +31 303 200 001