Delivering TRUST to the Digital World

VASCO®

Foreword

Most of us today live in an ever connected mode. If you are anything like me, you know you do live a digital life. Ask yourself: do you grab your smartphone immediately after waking up in the morning? Does leaving the house without it sound like a nightmare? How many laptops and tablets do you have at home? We bank online, interact online, make doctor's appointments online, read books and even meet new friends online.

In the digital world, Personally Identifiable Information (PII) which includes such distinctions as financial accounts, credit card numbers or even Internet Protocol (IP) address is a highly valued commodity. Safeguarding that information, therefore, has become a top priority.

Still, fraud is everywhere. So too the threat coordinators, hackers and cybercriminals that make a living in propagating it. As a result, living in a digital world demands trust. Trust in users, platforms, applications and devices. However, in this increasingly challenging environment one of the biggest issues facing information security professionals is that the traditional trust model is broken. (1)

Today, multi-factor authentication alone is not enough to ensure security. Instead, it requires a shift in mindset from securing individual unconnected pieces to delivering TRUST, holistically and organically, to the digital world. In fact, as this whitepaper suggests, trust is developed incrementally, recurring at each stage of a transaction between a user and a device. So, how can IT professionals and consumers benefit from digital trust?

It is easier than you might think.

Will LaSala

Director of Services @ VASCO

1. Forrester Research: https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682

What is Trust?

So, how do you define trust? According to the dictionary, “Trust is a firm belief in the reliability, truth, ability or strength of someone or something.”

In the context of security and technology, however, trust is formed between:

- Users and Client Applications
- Client Applications and Server Applications
- Server Applications and Users

When trust exists between these components, users can be allowed to do more. For example, users can be trusted to access more features within mobile apps that would not be available to them otherwise for security reasons (e.g. signing mortgage paperwork, sending a wire transfer, or opening a bank account).

As ‘Netizens’ we want to have more control and more trust in the digital world. Consider these recent statistics from Pew Research: (2)

93% of adults say that being in control of who can get information about them is important.

90% say that controlling what information is collected about them is important.

6% of adults say they are “very confident” that government agencies can keep their records private and secure.

6% of respondents say they are “very confident” that landline telephone companies will be able to protect their data and that the records of their activities will remain private and secure.

9% say they are “very confident” that data stored with Credit card companies will stay private and secure.

At the same time, Americans also value having the ability to share confidential matters with another trusted person. Nine-in-ten (93%) adults say this ability is important to them.

2. Pew Research Center’s Privacy Panel Survey, 1/27/2015 http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Mobile and the Trust Factor

Today, mobile devices as a means of paying for goods and services continue to accelerate throughout Europe, in North America and especially in Asia/Pacific where projected growth in mobile payments between 2014-2016 may exceed more than 20 million users a year. (3)

In Europe, for example, the number of mobile payment users between 2009 and 2010 nearly doubled, growing by nearly 8 million users in 2011 and well on its way to eclipsing nearly 9 million users year over year. In North America, from the period 2011-2014, mobile users grew by 40 million with another 30 million additional users projected by the end of 2016. Research indicates similar patterns of growth in Asia/Pacific, Africa, the Middle East and Latin America regions throughout the balance of 2016.

While mobile is the central point of the user ecosystem and users want it to do more, they mostly can't TRUST it. And here's why:

In a recent report (4) testers determined 95% of mobile applications were vulnerable. This includes:

- 6.5 average number of mobile vulnerabilities per application
- 35% had critical issues
- 45% had high risk issues

For 90% of those applications, testers were able to expose sensitive information, including cardholder data, usernames and/or passwords, personally identifiable information (PII) and even source code, the same information that has become highly valued commodities by cybercriminals.

It's no surprise that the mobile phone is bringing new demands such as a need for platform security and a further need for a server-based risk management platform.

Among user and application security trends associated with mobile devices, the market is looking for frictionless and password-less authentication and transaction data signing. In some circles, biometrics is gaining traction, but privacy issues remain a concern in some countries. There is also a merger of online fraud detection market with authentication and fraud prevention.

Significantly, regulations are evolving and addressing new markets including:

- **eBanking**: Local regulations, EBA, FFIEC
- **eGovernment**: eIDAS
- **Healthcare**: EPCS, eIDAS
- **eCommerce**: PSD2, XS2A, eIDAS

Ultimately, a proper and responsive mobile security solution must provide both end-to-end trust and security as well as ease of use.

3. Pymnts.com http://www.pymnts.com/in-depth/2015/mobile-transactions
4. Trustwave Global Security Report 2015: https://www2.trustwave.com/GSR2015.html

So, where do you need trust?

As we've seen achieving trust is not, at least initially, conferred only once. It occurs throughout the transaction chain:

1. You need to trust that you **know your user**

2. You need to have trust to **securely provision that known user with a strong credential that is easy to use for authentication**

3. You need to trust that the **device(s) are secure**

4. You need to trust that the **application is secure**

5. You need to trust the **communication channel** to/from your trusted identities, devices and applications

6. You need to trust the intent of the user whether it's a **financial transaction or process assurance** as information is exchanged

7. You need to trust the **user's behavior on all his devices across all of your channels**

With trust between these components, users can be allowed to do more and be trusted to access more additional features. In technical terms, trust is delivered via identity proofing, multi-factor authentication, mobile application security, fraud prevention, and digital signing. Need a further incentive to protect mobile transactions?

Consider the truism that trust takes years to build, seconds to break, and forever to repair.

> Trust takes years to build, seconds to break, and forever to repair.

What are the five technologies behind online Trust?

In the physical world trust, they say, is earned. That's also true in the online world where trust is incrementally earned at each touchpoint in a transaction. This includes:

1. **Identity proofing** (are you really who you say you are)

2. **Multi-factor authentication** (can the user you've presented be confirmed and validated through available authentication methods)

3. **Platform security** (is the platform [device and application] you are using to conduct the transaction known to be trusted)

4. **Transaction security** (is the exchange of data and the process used to exchange that data between you and a recipient trustworthy)

5. **Risk management** (is your online behavior, monitored throughout subsequent transactions, reliable and consistent or evasive and suspicious).

The key modules to delivering a platform built on TRUST

Trusted Identity Module

Delivering a platform built on trust starts, almost naturally and logically with a user. Ask yourself: are you absolutely and unconditionally certain your user is who you think it is? There are, of course, billions of potential users and only a very few of them can or should be yours. How do you distinguish this user? By their user name? By application type? How about their mother's maiden name? Maybe even, having them satisfy a credit check? Alternatively, you could start by proofing the identity of your user, electronically, using the identity proofing feature of VASCO's MYDIGIPASS solution.

MYDIGIPASS is a one-stop shop solution that offers electronic identity proofing, credential provisioning, secure login and fulfilment – all aspects of digital identity management in the cloud through a self-service portal.

MYDIGIPASS™

Are you sure that is who you think it is?

Trusted Credential Module

Once established, a trusted identity can be bound to a credential to prove ongoing trust in that identity. In order for such an identity-bound credential to be trusted, it must be provisioned to a secure device, such as a DIGIPASS GO 7 authenticator or a moble application on a trusted platform. The point of credential trust should be established when the user is in possession of the trusted device, whether through physical shipment of the hardware authenticator (delayed trust), or through establishment of trust in a mobile device and application, with subsequent delivery of a credential to that trusted application (immediate trust). Once this identity-bound credential is established, proof of posession of the trusted device can establish trust in the identity.

DIGIPASS is VASCO's family of user facing devices that offer secure provisioning and secure platform for both hardware and software options. DIGIPASS GO 7 is a FIPS 140-2 Level 2 Certified one-time password (OTP) hardware authentication device. DIGIPASS for Mobile is mobile authenticator that supports similar functionality on a mobile platform, offering ease of use for those verticals that allow mobile tokens.

Trusted Device Module

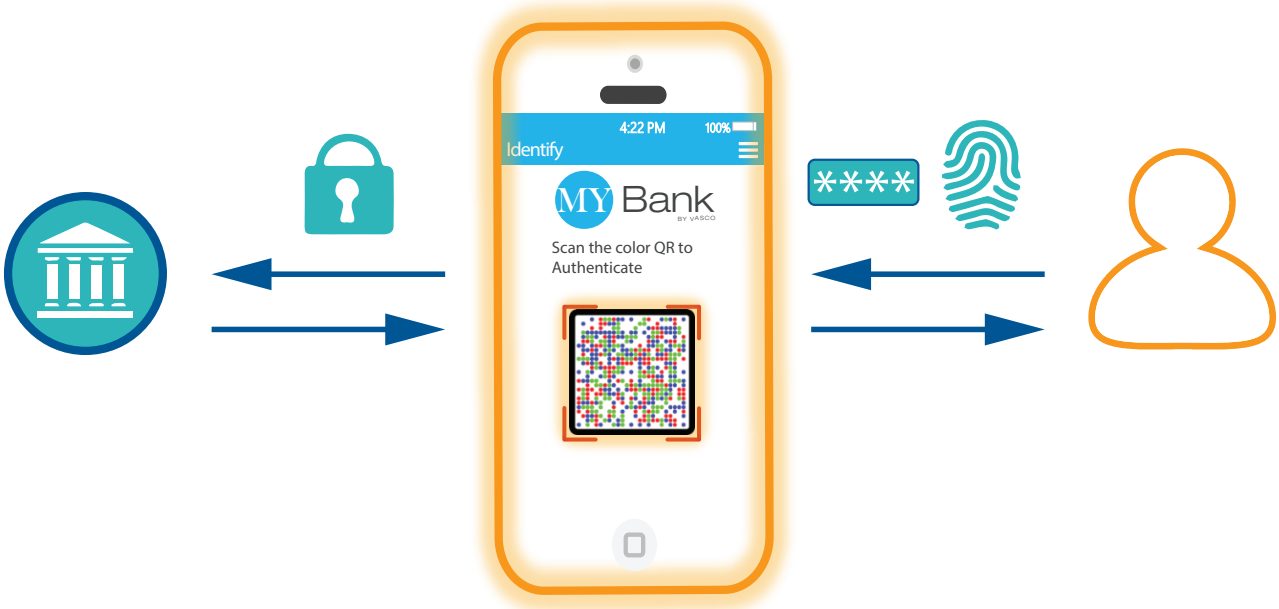
In some cases, the trust in the device is inherit, but in other cases, you must build that trust. Since you have already built the trust in the user, leverage that user to perform the process to trust the device.

The process of exchanging the trust from the provider and from the user to the potential device requires a comprehensive plan. The provider must create a secure channel to the device. The user must authenticate themselves to the device and to the provider. The device must then identify itself and prove that it is secure and has not changed. The device binds itself to the provider and the user and establishes a formal secure channel for future trusted events.

Now you have a trusted device.

DIGIPASS for APPS is a comprehensive software development kit (SDK) that natively integrates application security, multi-factor authentication and electronic signing into your mobile applications DIGIPASS for APPS offers a mobile. device binding feature as part of its mobile application security module.

DIGIPASS
for APPS



Trusted Application Module

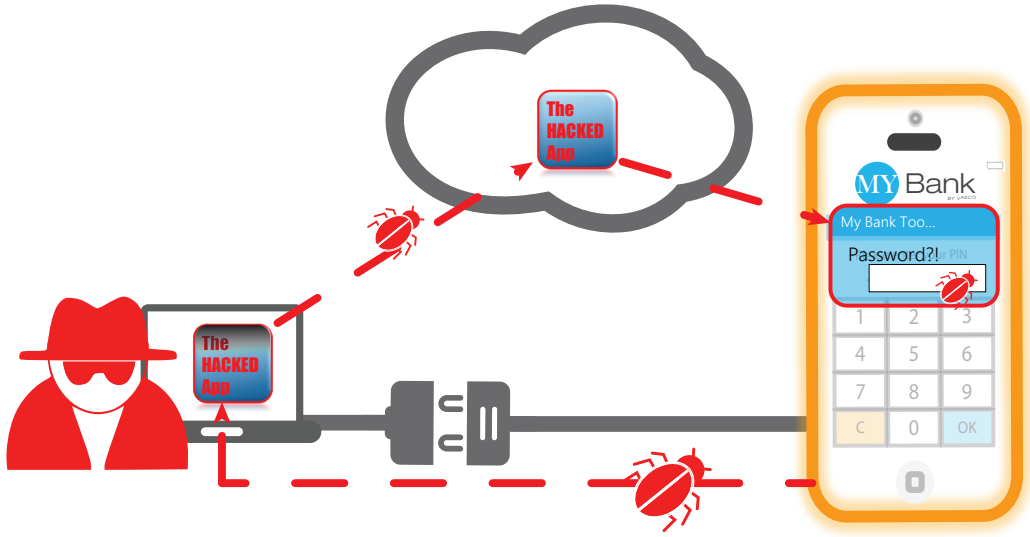
Next, ensure that the application is secure by using technologies like RASP (runtime application self-protection). **Runtime Application Self-Protection (RASP) security** provides a high level of protection for mobile applications even if users inadvertently download malware onto their mobile device. By providing RASP technology with DIGIPASS for APPS, VASCO protects the integrity and trust of mobile applications to ensure that data and transactions are not compromised.

The VASCO DIGIPASS for APPS Runtime Application Self-Protection security module ensures the integrity of a trusted platform in three ways, Protect, Detect and React. RASP will protect the trusted mobile application by providing Code Obfuscation techniques. During the detection phase of RASP, VASCO will detect malicious keyboards, screen readers, repackaged applications, debuggers and emulators, and jailbroken or rooted devices. RASP will offer the application a way to react to prevent screenshots, block screen duplication, custom reactions and it will provide alerts or the ability to shut down the application.

Remember, you already have a trusted digital identity of your user as well as a trusted device bound to that user. Now you also have a trusted application.

DIGIPASS for APPS RASP component allows you to extend and strengthen application security, deliver unprecedented convenience to your users, and streamline application deployment and lifecycle management processes.

DIGIPASS
for APPS



Trusted User Module

When your users start to live their digital lives, you allow the trust you have built to continue. For every online or mobile session, the user must prove their trust, which now means simply proving they have completed the previous trust platform steps. If something raises a red flag, a higher level of security, such as multi-factor authentication, will be required. However, this is not the case in every instance, thereby avoiding unnecessary burden on users.

Leveraging the DIGIPASS for APPS components, your mobile application can be tasked to ask for further trusted authentication when required or requested due to enhanced security needs for different levels of access. In some cases, a simple "Something you know" factor of authentication can be leveraged, and trusted to allow access to non-sensitive tasks and data. In other cases, stepping up your authentication to include a "Something you have" factor of authentication along with the previous factor, will provide true two-factor authentication. Two-factor authentication ensures that sensitive data is protected in your trusted environment. Finally, leveraging the "Something you are" factor of authentication can be added to the entire process to help ensure the highest level of authentication security while maintaining an ease of use and a true trusted platform.

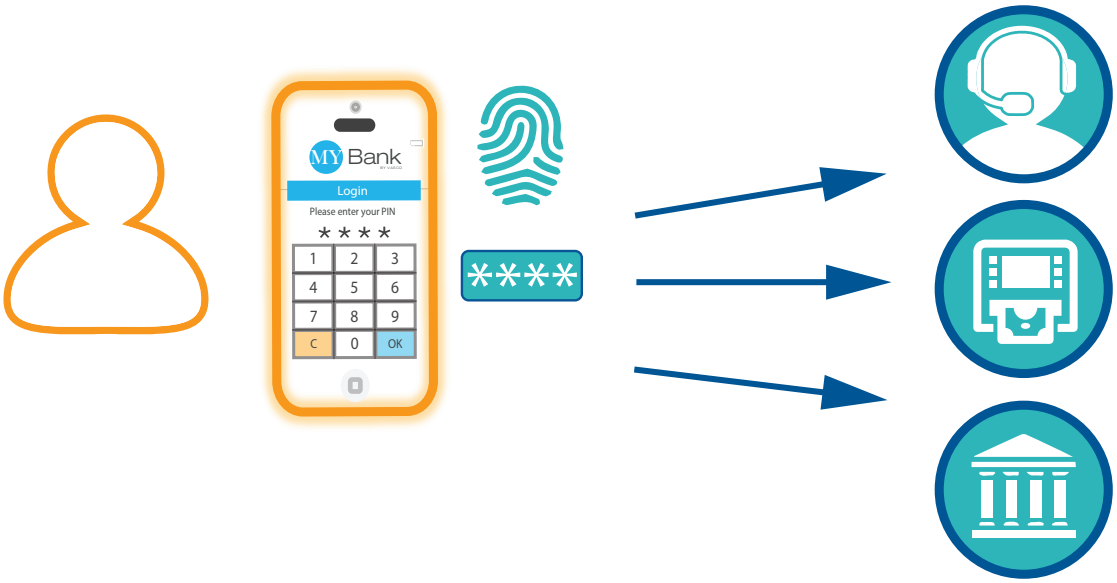
DIGIPASS is VASCO's family of front-end authentication devices and applications. From software to hardware to biometrics, all DIGIPASS family is supported on the same platform and can be mixed and matched to ensure positive user experience.

Static Password | Voice & SMS Token | Hardware Token | Software Token | Wearable | Biometrics

Trusted Intent Module

Once the user leverages a trusted device from a trusted platform, the INTENT of the user should also be trusted. This can be done with the use of transaction authentication — a cryptographic solution that demonstrates the authenticity of a digital message or transaction. It gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit. As a result, the recipient is provided with message authentication, non-repudiation and integrity. Users want their intent to be trusted easily, securely and by whatever device is handy. Each of these complex protocols can be implemented behind the scenes using VASCO's IDENTIKEY Authentication Server and VACMAN Controller.

VASCO's IDENTIKEY Authentication Server is a World Class Triple A Authentication platform with comprehensive interfaces for Administration, Helpdesk and End user self-management for all authentication needs. IDENTIKEY Authentication Server and all of VASCO products are built off VASCO primary authentication library, VACMAN Controller. This Software Development Kit can be embedded into any platform and can make any application DIGIPASS-Ready.

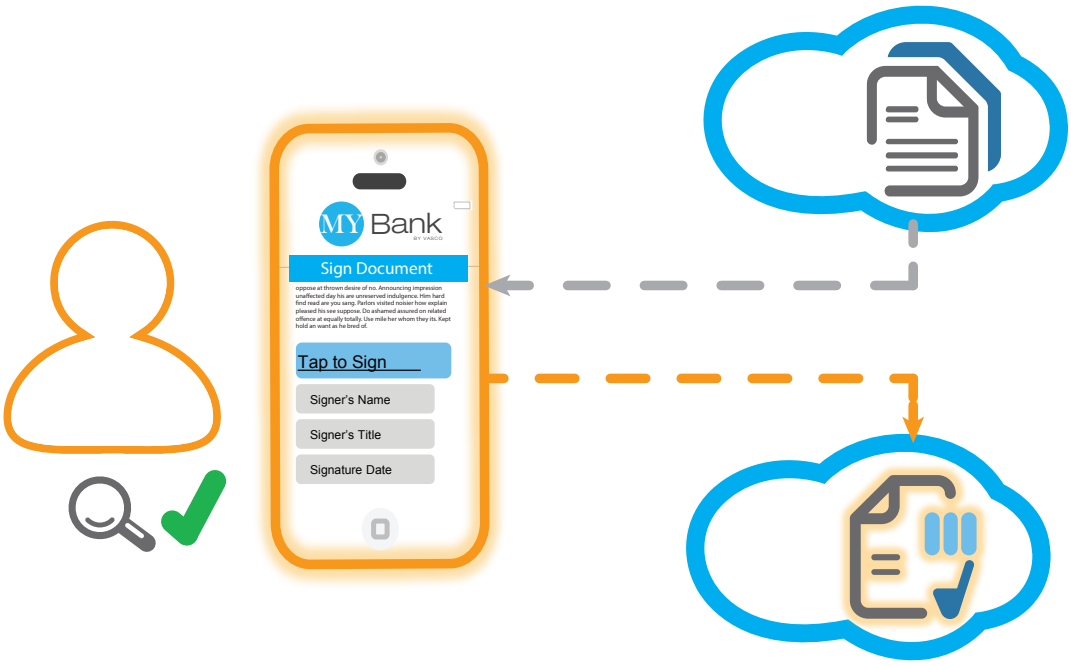


Trusted Transaction Module

After you have established a trusted identity, trusted device, trusted application, and trusted user intent, you can actually USE the trusted platform you have built to automate more customer services such as customer onboarding, purchase orders, document signing, expense reports, etc. Anywhere a trusted electronic signature is needed for compliance and convenience; it can be done with eSignLive by VASCO.

eSignLive is VASCO's e-signature solution for secure document signing processes. eSignLive gives consumers the ability to perform a myriad of activities online and securely including, for example, applying for life insurance, closing on a mortgage, opening a new bank account or signing a sales contract on their own terms – at the time, place and on the device of their choice.

eSignLive™ by VASCO

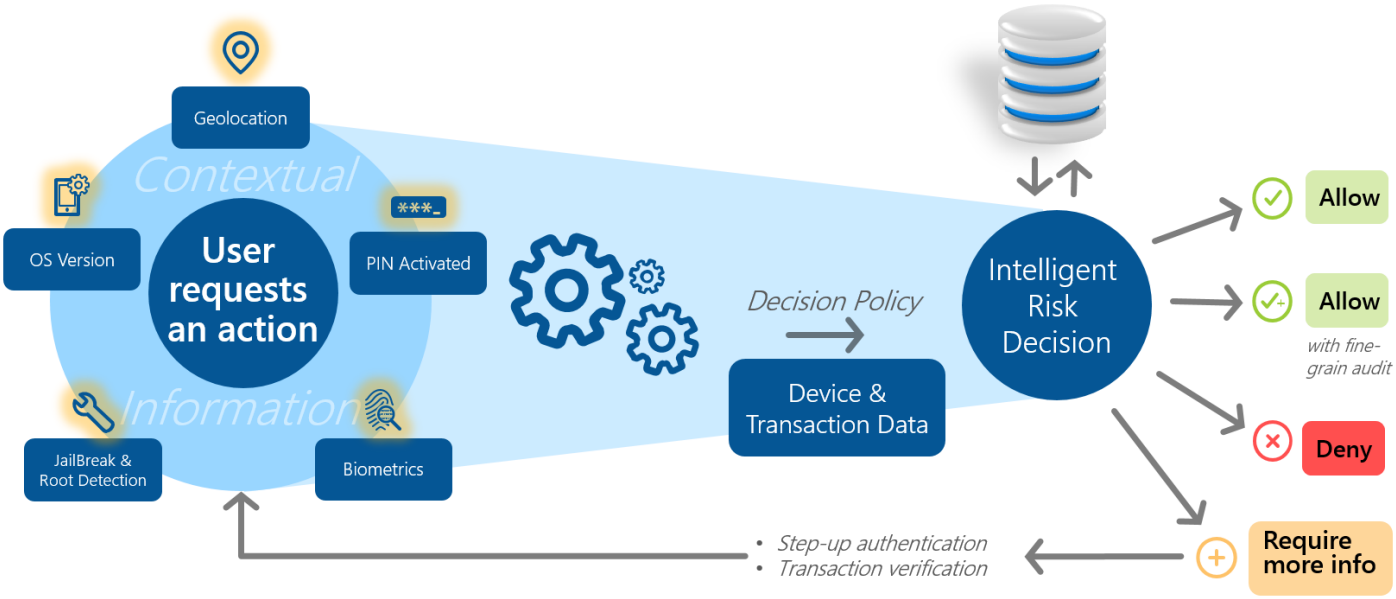


Trusted Behavior Module

The final step is to look at what the user is doing, in real time, and how they are doing it to ensure the trust has not been broken. In other words, trust continues to be earned throughout the digital journey of your customer. Ensure that trust has not been broken by using VASCO's IDENTIKEY Risk Manager Platform.

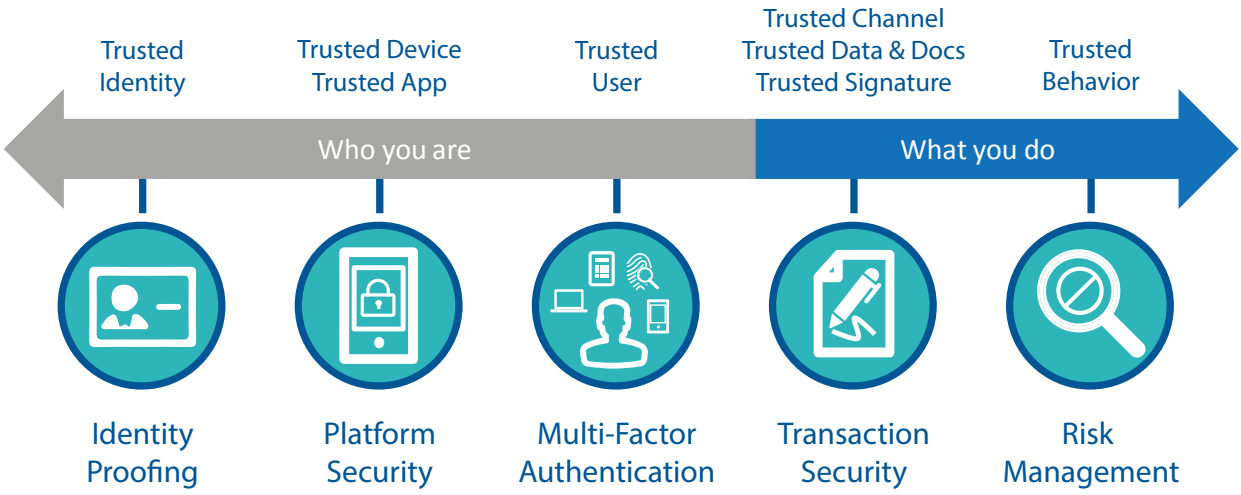
VASCO's IDENTIKEY Risk Manager collects the trusted platform details, intentions, process and transactions and processes the data to look for anomalies. The IDENTIKEY Risk Manager will add additional data points to the analyzed and collected data, and in real-time, it will allow you to take action on the results. The action could be to step up authentication for the end user while they are interacting with your platform. Alternatively, the action could be to further collect and prevent attackers from getting into your trusted platform.

VASCO IDENTIKEY RISK MANAGER (IRM) is a comprehensive fraud detection solution designed to help you improve the manner and speed at which your organization detects fraud across multiple channels, enabling you to take a proactive approach to fraud prevention, while at the same time making the experience as painless as possible for your users.



Trusted Platform

VASCO is a recognized leader in mobile application security, multi-factor authentication, electronic signatures, and risk management solutions to businesses and government agencies in over 100 countries worldwide.
The illustration below demonstrates VASCO's holistic approach to creating and maintaining digital trust throughout a customer's mobile and online journey.



Conclusion

The incremental steps described in this document enable a secure digital platform delivering much needed trust to the digital world: to your employees, to your customers and to your partners. As a result, you can enjoy this digital trust at work, at home, and on the go, no matter what you do, bank, buy a house, get an insurance policy, exchange pictures with friends or meet new people. A trusted digital identity created and fostered by the multitude of new technological advances will soon become the medium not only to facilitate security but also to improve user experience. Equipped with trusted digital identities, employees and consumers can be allowed to do more, in a quicker fashion. Essentially, VASCO helps you secure who you are and what you do.

VASCO helps you secure who you are and what you do.

About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit www.blog.vasco.com