i-Sprint
Trust without Boundaries

Developing Your Authentication Strategy

i-Sprint's Multi-Factor, Versatile Authentication for Different Use Cases

Issue 2

Featuring research from
Gartner

Introduction

In our last newsletter issue "Simple, Strategic and One Login for Enterprise, Cloud and Mobile", we discussed about today's Single Sign-On (SSO) landscape and why a serious evaluation of SSO solutions is essential to all enterprises. SSO helps enterprises increase productivity, enhance security and reduce support costs in today's business landscape and the benefits of an SSO initiative outweigh the absence of it.

Still, a nagging concern persists. If the single credential is compromised, an attacker has free reign over all accessible resources. We need to ask ourselves, does the universal simple password, which can be easily cracked, provide adequate authentication in an SSO world.

Password has been the preferred authentication mechanism for many years. Whether passwords provide sufficient security has everything to do with what is being protected.

Source: i-Sprint Innovations

Today's Threat Landscape

Data Explosion

- 1,800 billion gigabytes of data produced by humans in 2011. [i]
- IBM says we are producing 2.5 quintillion bytes of data per day. "There are expected to be one trillion new devices connected to the internet in the near future, which will help drive 44 times digital data growth by the year 2020..." [ii]

How Safe Are Your Data?

The threat environment is moving exponentially. In the last year, we have seen reports in the press from government entities to major online companies and brands, experience data breaches and password compromises. The username-password combination as an authenticator does not work any longer. The cases of database breaches over the last year have compromised tens of millions of records. The pace of security breaches has not decreased despite advances in security measures and intrusion prevention technologies. According to statistics compiled by Internet Crime Compliant Center (IC3), the total monetary loss that was incurred due to hacking attempts is $525,441,110.00.[iii] This is an alarming insight into the financial scope of the problem.

On 3rd October 2013, Adobe released an official announcement that "certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders"[iv] have been compromised. The most costly password hacks are wholesale thefts of an organization's entire database of customer and/or employee user IDs and passwords. Armed with the stolen information, criminals can then quickly reap data or money. Whether the motivation was financial or espionage, the results are devastating.

Cost to Businesses

Compromised credential management processes result in the need to re-issue credentials, which can be an expensive and time-consuming process.

Credential validation rates can vary and can easily outpace the performance characteristics of a credential management system, jeopardizing business continuity.

Business application owners' expectations around security and trust models are rising, and can expose credential management as a weak link that may jeopardize compliance claim.

According to 2013 Data Breach Investigations Report by Verizon, victims of breaches span across industries across the globe but with a higher percentage from financial organizations and larger organizations.

of breaches affected financial organizations (+)

of breaches occurred in retail environments and restaurants (-)

of network intrusions involved manufacturing, transportation, and utilities (+)

of network intrusions hit information and professional services firms (+)

of breaches impacted larger organizations (+)

different countries are represented

Source: Verizon, 2013 Data Breach Investigations Report, Who are the victims?

In the same report, we also see that 76% of network intrusions exploited weak or stolen credentials.

used some form of hacking (-)

of network intrusions exploited weak or stolen credentials (-)

incorporated malware (-)

involved physical attacks (+)

leveraged social tactics (+)

resulted from privilege misuse and abuse

Source: Verizon, 2013 Data Breach Investigations Report, How do breaches occur?

Legend:

- A plus (+) sign indicates either a 10% or greater increase from the previous year's report
- A minus (-) sign indicates a 10% greater decrease from the previous year's report
- Measurements without an indicator showed no significant change

Source: i-Sprint Innovations

i The Futures Company, Privacy, From Data to People, 2012

ii DMH Stallard, Secure Your Data – Protect Your Business, June 2012

iii "IC3, 2012 Internet Crime Center Report, May 2013

iv http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html

New Vulnerabilities

Mobile Threats

Worldwide sales of smartphones (12% growth) and tablets (18%) will continue at a significant pace, accounting for over 60% of total IT market growth[i]. Android remains the world's most widely used operating system used by hundreds of millions of customers worldwide. In a joint unclassified memo from the U.S. Department of Homeland Security and Department of Justice, an overwhelming 79% of all mobile malware threats target devices running on Google's Android operating system[ii].

In recent months, **Android Master Key Vulnerability**[iii] has been a rising concern for Android users. It allows attackers to take a legitimate app, change the contents of that app, and republish it on third-party marketplaces without changing the signature of the original application produced by the original vendor. Rogue apps purporting to be a mobile banking app for a bank have been reported in the third quarter of 2013.

Attacks on Two Factor Authentication Systems

Online applications are increasingly exposed to middleman attacks like Man-in-the-Middle Attack (MitMa), man-in-the-browser (MitB) attack, Man-in-the-Mobile (MitMO) attacks and it is important to implement measures to minimize exposure to such attacks.

Brute Force Attacks on Password Hashing Schemes

Traditionally password hashes have been used to protect the passwords in storage. But with the availability of affordable consumer graphics cards, a $500 GPU (Graphics Processing Unit) can be used to decrypt tens of millions of hashes per second. This increases the risk of brute force attacks by insiders or by hackers who may have gained access to the password database.

Bring Your Own Device (BYOD)

The widespread adoption of smart phones, tablets and laptops to access company networks and data has introduced a whole new world of vulnerability challenges for IT security professionals. Organizations are starting to implement corporate security policies for BYOD. Research firm J. Gold Associates reports that about 25%-35% of organizations currently have a BYOD policy, and they expect that to grow to over 50% over the next two years[iv]. Consumers and employees now have continuous connectivity. Consequently, a significant amount of sensitive corporate data such as business email, customer databases, corporate presentations and business plans, are making its way onto these devices.

With the increased number of employees bringing their own devices and working remotely, mobile devices are playing a huge role in authentication methods and scenarios, and consequently, cloud-based authentication services are also on the rise. The expanding use of cloud-based IT services and the increasing popularity of apps such as online banking mean that IT needs to pay closer attention to authentication.

Source: i-Sprint Innovations

i http://www.forbes.com/sites/gilpress/2013/12/03/idc-top-10-technology-predictions-for-2014/

ii http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf

iii http://www.scmagazine.com/threat-of-the-month-android-master-key-vulnerability/article/307403/

iv http://searchconsumerization.techtarget.com/tip/Mobile-device-strategy-bypassed-as-enterprises-face-tablet-invasion

The Impact on Authentication

So we see that the rapid growth of mobile devices that can access corporate networks and data, and the increasing popularity of apps such as online banking have triggered organizations to re-evaluate their strategies and pay closer attention to authentication. Two main trends are having an impact on authentication. One is the increasing frequency of security breaches that expose user passwords, personally identifiable information and other high-risk data that has high financial, commercial impact or affecting national security. The other is the ubiquity of mobile devices.

> Businesses are turning to stronger authentication. They must drive the nimbleness demanded by employees and customers, while ensuring they do so securely.

Ubiquity of mobile devices

The ubiquity of mobile devices means that any authentication mechanism deployed must be compatible with mobile access. This has posed a hindrance to the traditional hardware PKI tokens based deployments. With the adoption of smartphones, there is an increased interest in using the mobile phone as the authentication device with the advantage of being able to provide a better user experience.

Managing Risk

Organizations are providing different kinds of online services with different risk levels. Access channels could be IVR, Desktop based access, Mobile access, ATM, Kiosk or Branch. The authentication mechanism deployed should commensurate with the risk level of the service. At the same time, different types of users have different usage profiles (access device, frequency, roles, personal preference).

All this leads to a need to have the capability to be able to support a variety of authentication mechanisms.

Choice of Authentication Mechanisms

Enhanced methods of authentication have morphed from traditional tokens to USB devices to smart cards to fingerprint readers, soft tokens and scanning devices. Contextual authentication, based on analytics of behaviour patterns and device patterns, is growing in importance and more vendors are offering it with their core user authentication products. Additionally, there is an increased interest in using biometrics for a higher level of assurance with improved user experience, including form factors like typing rhythm, voice recognition, face topography and iris structure.

Cloud-Delivered User Authentication Services

Move to cloud-delivered user authentication services are becoming more widely adopted and having the most traction among small and mid-sized businesses and industries where total cost of ownership (TCO) is a more significant consideration.

Source: i-Sprint Innovations

What should be your Authentication Strategy?

Given the above trends and challenges, IT Architects are faced with the question of how to address the COMPLEXITY of managing multiple mechanisms, at a reasonable CAPITAL and OPERATIONAL cost and yet have AGILITY in responding to changing needs for Authentication?

We recommend investing in a Versatile Authentication Server and more importantly to decouple the authentication backend from the authentication device vendor.

Source: i-Sprint Innovations

The i-Sprint Solution: AccessMatrix™ Universal Authentication Server (UAS)

Understand and evaluate the threat landscape and prioritize a treatment strategy.

Don't buy into a "one-size-fits all" approach to security.

Multi-Factor Authentication

Now that we understand the threat landscape and its implications to businesses, implementing Multi-factor Authentication to corroborate that the user is who he claims to be, is an important focus for every business today.

Multi-factor authentication can be defined as requiring two or more of the following factors:

- What you know: such as a password
- What you have: like your ATM card / OTP token
- What you are: biometrics characteristics such as your fingerprint, voice or facial recognition
- Where you are: contextual authentication, based on the analytics of behaviour patterns and other information of a user

Multi-factor authentication requires the user to exchange a single credential for two or three more times. You may require Level 1 authentication (simple password) to access the computer and network, while requiring Level 2 authentication (one-time password or smart card) to access human resources or financial data. For sensitive applications, you may add biometrics into the mix. According to Gartner, "By 2015, 30% of users accessing corporate networks or high-value Web applications from smartphones or tablets will use biometric authentication, up from less than 5% today."[1]

Multiple Authentication Methods for Different Use Cases

As organizations seek new, risk-appropriate user authentication methods, it is a point to note that a single authentication method is rarely appropriate across all use cases. In re-strategizing, most organizations tend to base their decisions on a single use case. According to Gartner, "As use cases have different needs and constraints, a single authentication method is rarely the best fit for multiple use cases within the enterprise. This can have two consequences:

- Implementation of redundant solutions, with unnecessary cost and complexity
- Reuse of an incumbent method in new use cases where it may be a less-than-good fit, unacceptably reducing security or unnecessarily increasing TOC and over burdening users"[2]

Future Proof Versatile Authentication Solution

Through a single, unified framework, i-Sprint's AccessMatrix™ Universal Authentication Server (UAS) enables organizations to deploy a wide variety of authentication methods to achieve strong authentication and benefit from evolving authentication mechanisms.

A future-proof versatile authentication infrastructure, UAS supports multiple authentication mechanisms for strong authentication requirements, enabling organizations to rapidly deploy those selected authentication methods that address their specific requirements.

UAS supports a wide range of authentication methods using a Pluggable Authentication Module (PAM) approach and new ones can be easily added to cater for evolving authentication mechanisms. Organizations can also use the authentication workflow to chain two or more authentication methods for strong authentication and authorization requirements.

The out-of-the-box end-to-end token & biometrics life cycle management module greatly streamlines the administration and reduces time-to-market.

With our patented Segmented Hierarchy-Based Security Administration and Authorization Framework, UAS allows organizations to designate security administrators at different levels of the organization. The framework can be extended to allow external organizations to manage IDs and user rights by their own security administrators. This feature has been proven to be well suited to address administration requirements for Management Security Providers or SaaS Providers.

End to End Encryption of Static Password

Two Factor Authentication is typically a combination of static password and other mechanisms. While organizations look at implementing the second factor mechanism, it is important not to forget to adequately protect the static password.

UAS provides a module to end-to-end encrypt the static password from the point of entry (browser) to the point of comparison (inside a FIPS certified HSM). This ensures that no one within the organization has access to the password in clear protecting against internal fraud.

AccessMatrix™ Universal Authentication Server (UAS) Features

Reduce operational cost with a common scalable versatile authentication and token management solution that supports different use cases

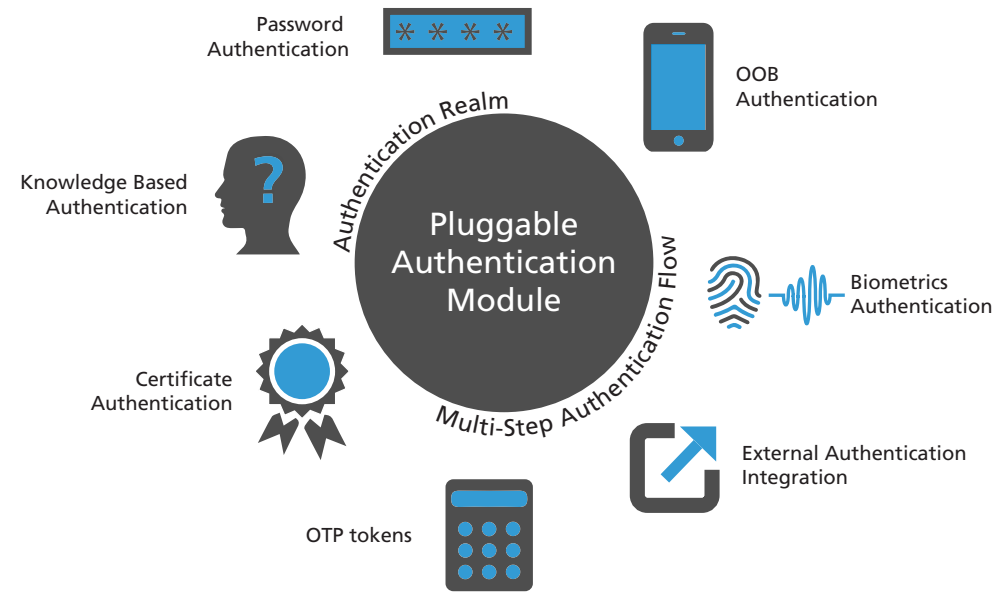
Simplify integration and deployment efforts with ready PAM modules and native integration with existing LDAP, AD and JDBC directories.

Handle complex authentication requirements with flexible and dynamic authentication workflow

Cater for future authentication options with the PAM framework of our standard-based versatile authentication solution which enables new authentication methods that can be added with minimal impacts to existing strong authentication deployments.

Provide a highly scalable, open and reliable platform to support demanding operational requirements such as automatic failover, horizontal and vertical scaling and round-the-clock operations.

FIGURE 1 Supports Multiple Directories, Multiple Factor & Multiple Steps Authentication Methods



AccessMatrix™ UAS Modules

UAS offers a wide range of ready and customizable authentication options to meet the strong authentication options to meet the strong authentication requirements for enterprise and customer-facing applications.

UAS – End to End Encryption Module

- User Credentials, with Pin Mailer Generation
- Data in Transit
- ATM PINs, with ISO9564 based translation

UAS – OTP Token Authentication and Life Cycle Management Module

- OOB OTP
- SafeNet Tokens
- RSA Tokens
- Taiwanese FISC-II Tokens
- Vasco Tokens
- DynamiCode Tokens
- OATH Tokens

UAS – YESsafe Mobile Tokens

- YESsafe Mobile Token provides key token features for Authentication (Both Synchronous and Challenge Response), Authorization, Signature Verification and host return code.

UAS – Fingerprint Biometric Authentication and Management Module

UAS – 2FA for Enterprise Authentication Modules

- Windows Desktop Login using GINA & CP, Terminal Server and Citrix
- RADIUS for network devices, VPN & Unix Logins
- MS Outlook Web Access

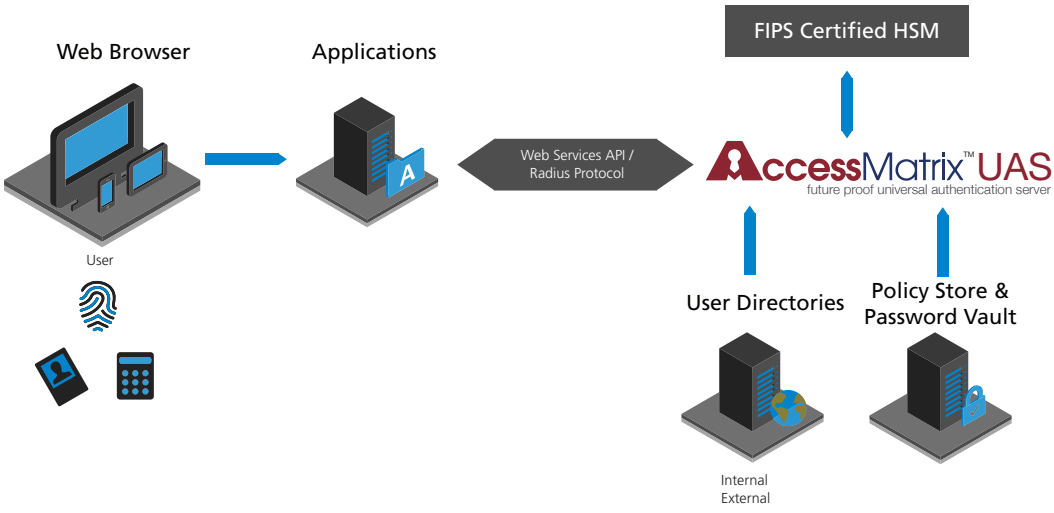
UAS – SDK for Application Integration

UAS – 2FA Integrations for Third Party WebSSO Products

UAS – HSM Integration Modules

- HSM Key Manager for protection of credentials in storage
- OTP verification inside HSM

FIGURE 2 AccessMatrix™ UAS Technical Architecture



Source: i-Sprint Innovations

[1-2] Gartner Inc., How to Choose New User Authentication Methods, G00249403, 27 March 2013

Case Study: End-to-End Encryption, Two Factor Authentication and Token Management Platform for the Strongest, Most Profitable Bank in ASEAN

The Bank needed a web-based Internet Banking channel to serve its Customers and Corporate banking clients in the Asia Pacific region. It must comply or exceed security guidelines outlined by all the central banks in the Asia Pacific region including the Monetary Authority of Singapore (MAS) and Hong Kong Monetary Authority (HKMA).

The Bank needed a total solution that provides:

1. End-to-end protection of customer PIN – The encrypted PIN must be encrypted from the point of entry (browser) to point of comparison (inside a Hardware Security Module). The customer PIN must also be protected throughout the process of creation and printing.

2. Strong authentication with One Time Password (OTP) VASCO token and OTP over SMS – this is also a requirement based on corporate security standards and internet banking regulatory requirements.

3. A common security solution to help them address the above two requirements in order to comply with the government regulations for Internet Banking applications. The solution must provide the administration and management functions to handle distribution and management of hardware tokens.

i-Sprint's security consolidation methodology was applied throughout the project to assist the bank to implement and deploy AccessMatrix™ Universal Authentication Server (UAS) End-to-End Encryption Authentication (E2EEA), VASCO Token Management Module and SMS OTP Module to provide the authentication backend and management platform for the bank to achieve the authentication and administration requirements to comply with the banking regulations for internet banking.

AccessMatrix UAS E2EEA provides a total solution for PIN life cycle management including secure pin generation, pin mailer printing. The Pin is encrypted on the endpoint (PC or Mobile) using UAS Client side encryption libraries and remains encrypted till the point of comparison inside an HSM. This ensures that no one within the bank has access to the PIN in clear.

AccessMatrix™ UAS VASCO Token Management Module also provides seamless integration with the Bank's existing ActivCard OTP tokens which enables the Bank to protect their existing investments without any interruptions. UAS VASCO Token Management module also provides out-of-the-box solution to leverage all the security functions provided by the VASCO DigiPass Tokens. The pre-integrated and tested 2FA solution reduces integration complexity and shortens the time to deployment for 2FA for security sensitive applications for strong authentication requirements. The Integrated solution also enables the administering of the entire token management life cycle i.e.:

- Issuance (Factory Initialized or Self Initialized), Delivery, Enablement, Lost Tokens, Out of Sync and Replacement over time

- Customizable user interface to facilitate Help Desk staff to support token management functions

- Detail Audit Trail information and flexible reporting

- Customizable self-service interface for user to perform some token management functions

i-Sprint's AccessMatrix™ Universal Authentication Server platform helps the Bank in promoting confidence and integrity of access across its e-channels. The platform also laid the framework of trust for a robust technology risk management process that is capable in handling all known attacks and provides a platform for a rapid response to future exploits. Last but not least, the platform provides the flexibility of allowing the Bank and its Clients to select a convenient yet secure Authentication risk-based approach of accessing its banking products.

Source: i-Sprint Innovations

Conclusion

The highly connected world that we are living in today and its global communications systems have triggered technological, social and cultural changes. This level of interconnectivity has introduced a diversity of risks that will remain vulnerable if enterprises do not take a serious assessment of their risks, and determine the appropriateness of authentication methods to use, and how they should be implemented.

Multi-factor authentication is a significant step in the right direction. Adoption of multi-factor authentication allows universal adaptability across a range of endpoints while maintaining a high level of security and reliability.

i-Sprint's AccessMatrix™ Universal Authentication Server (UAS) is a highly scalable versatile authentication server. Its support for multi-vendor authentication devices prevents vendor lock-in and lowers total cost of ownership.

Good security is about being proactive and mitigating risk. AccessMatrix™ UAS contributes flexibility and agility to an organization's authentication strategy leaving organizations to focus on innovation in serving its customers and driving efficiency for staff.

Source: i-Sprint Innovations

Research from Gartner

How to Choose New User Authentication Methods

Enterprises are seeking new, risk-appropriate user authentication methods, but a single method is rarely appropriate for all use cases. An IAM leader or security architect will likely need to choose a set of various methods to meet all the needs of the enterprise.

Key Challenges

- Most authentication buying decisions are tactical and focus on a single use case. IAM leaders and security architects are putting greater weight on total cost of ownership (TCO) and user experience (UX).
- Each use case has different needs and constraints. Thus, a single authentication method is rarely the best fit for all use cases within the enterprise.
- The adoption of mobile computing is multiplying the variety of methods used, but this trend is likely to be unsustainable in the midterm to long term.

Recommendations

- Consider TCO, UX and endpoint independence, as well as authentication strength, when evaluating new authentication methods.
- Assess how users, endpoints, locations and the assets being accessed determine your needs in each use case. Don't neglect regulatory compliance constraints and adjacent security needs.
- Define an optimal set of authentication methods that meets the needs of all use cases in the simplest way, but with minimum trade-offs. Identify appropriate ways of implementing them.

Strategic Planning Assumption

By 2015, 30% of users accessing corporate networks or high-value Web applications from smartphones or tablets will use biometric authentication, up from less than 5% today.

Introduction

Most authentication buying decisions are tactical and focus on a single use case. As use cases have different needs and constraints, a single authentication method is rarely the best fit for multiple use cases within the enterprise. This can have two consequences:

- Implementation of redundant solutions, with unnecessary cost and complexity
- Reuse of an incumbent method in new use cases where it may be a less-than-good fit, unacceptably reducing security or unnecessarily increasing TCO and overburdening users

How can enterprises optimize their choice of authentication methods and how they're implemented across multiple use cases?

This research outlines a decision framework that identity and access management (IAM) leaders, security architects and other practitioners can use to determine the optimal authentication solution across a range of use cases, providing a basis for vendor and product selection.

Elements of the framework can also be used:

- To review incumbent solutions
- For single use cases in isolation
- During the development or acquisition of new applications to identify which method in the optimal set is most appropriate (or whether a new method is needed)

Preamble

Authentication (see Note 1) is foundational to other IAM functions. Confidence or trust in a claimed digital identity is crucial to authorization (for example, segregation of duties) and intelligence (for example, auditing).[1]

A wide variety of authentication methods is available (see Note 2 and "A Taxonomy of Authentication Methods, Update").

Good authentication choices are characterized by:

- Risk-appropriate authentication strength[2]
- Low (justifiable and affordable) TCO
- Good (acceptable minimum) UX[3]
- Endpoint independence[4]

Overview of Gartner's Framework for Choosing New Authentication Methods

The decision framework has the following high-level structure:

- Identify all current and likely future use cases.
- Determine what authentication methods you will use.
- Determine how you will implement them.

The full framework is illustrated in Figure 1.

Note that this is not a simple linear process. Depending on the use cases considered and the choices that emerge from them, the two "legs" depicted in Figure 1 ("What methods will you use?" and "How will you implement them?") may not be independent, and each can influence or constrain the other. Some iteration will likely be required.

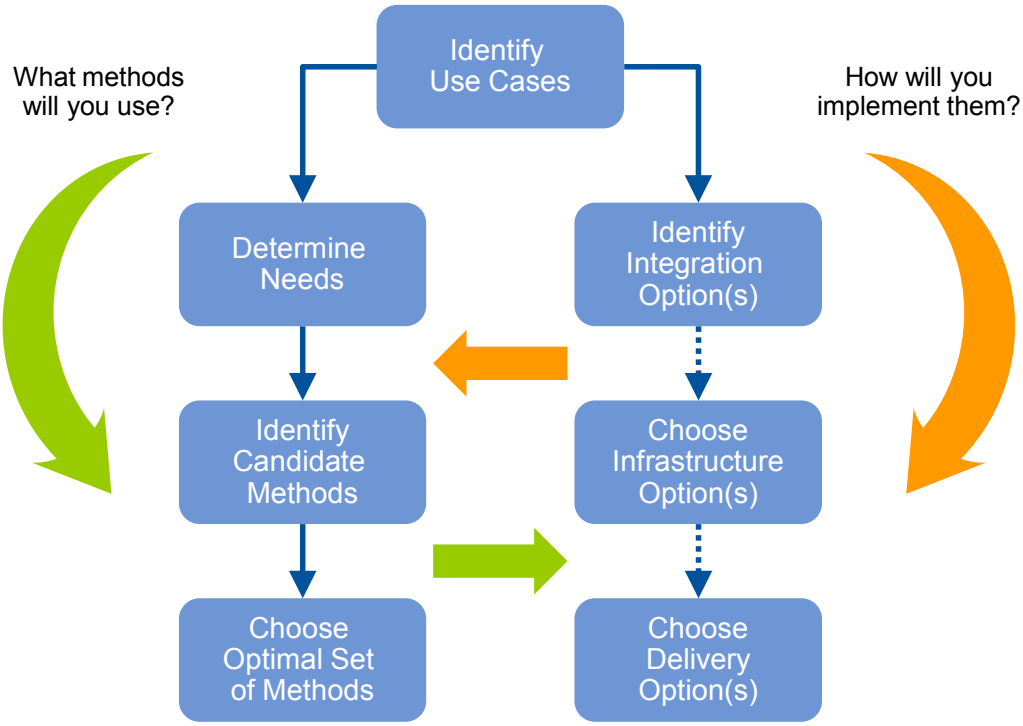
Analysis

Identify Use Cases

First, enumerate the different use cases for authentication. Note 3 outlines a set of use cases that we use in other Gartner research that might encompass the needs of your enterprise, but you might be able to identify others as well.

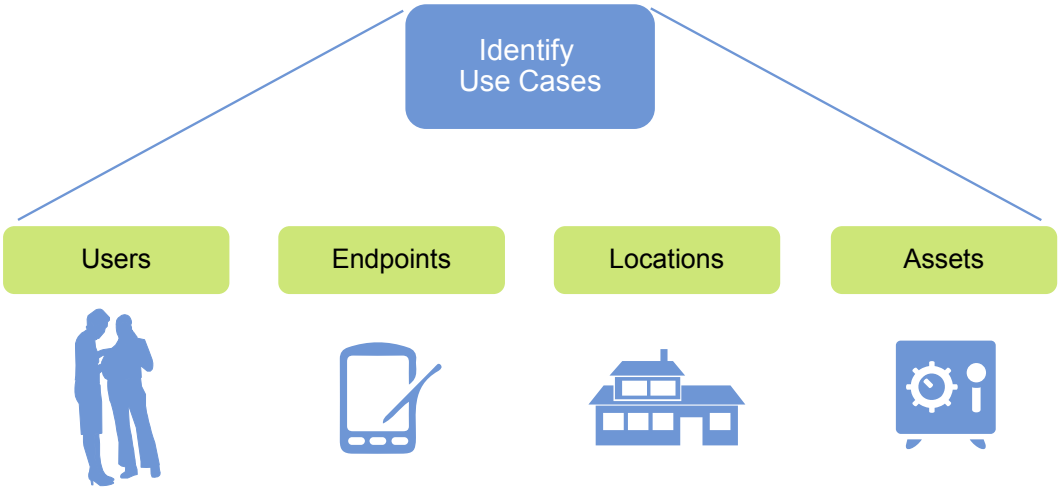
More important than this list are the characteristics that define and differentiate the use cases (see Figure 2).

FIGURE 1 Gartner's Framework for Choosing New Authentication Methods



Source: Gartner (March 2013)

FIGURE 2 Identifying Use Cases



Source: Gartner (March 2013)

Who Are the Users? How Do They Influence and Constrain Your Choices?

Consider these aspects:

- Relationship or constituency, which indicates acceptable constraints on (mis)behavior. While your workforce is bound to use the authentication method you impose, your customers (or any users with an elective relationship) don't have to. Poor UX has an impact on customer retention.[3]
- Presence, which impacts registration/enrolment and credentialing/provisioning. Logistical costs for geographically remote users are a particular concern.
- Numbers, which have a direct impact on TCO. Pricing for different methods scales differently.
- Other relationships, which might influence users' attitudes toward different methods.[5]

What Endpoints Are Used? How Do They Influence and Constrain Your Choices?

Consider these aspects:

- The variety of form factors and OSs that will be used. There may be technical restrictions on what methods can easily be used with what endpoints. For some authentication methods, UX or authentication strength can differ across different endpoints.[6]
- Ownership. Methods that require software or connected hardware components might not be acceptable to user/owners or third parties (such as business partners). Even if such components are acceptable, providing technical support on non-enterprise-owned devices can be problematic.

Where Is Access From? How Does This Influence and Constrain Your Choices?

Consider these aspects:

- Local or remote access. For local access, there may be controlled physical access to the endpoint, which can reduce risk and thus the target authentication strength.[7] Support for remote access can be problematic for some authentication methods.[8]
- Mobility. That is, do users get access from the same location, or do they move between local and remote locations or among different remote locations? If the answer is the latter, the method must be available across multiple locations. This can be a particular challenge for out of band (OOB) authentication methods, depending on vendor support and local mobile network operators.
- Signal strength. This varies according to mobile network coverage and a user's location within a building, and can place restrictions on OOB authentication.[9]

- Allowed devices. Restrictions on taking phones into certain locations, for security reasons or because of potential interference with sensitive equipment (for example, hospitals), can preclude phone-as-a-token authentication methods.

What Is Being Accessed? How Does This Influence and Constrain Your Choices?

Consider these aspects:

- The value or criticality of an asset is a leading indicator of risk.[10]
- The sensitivity of an asset may demand high accountability (rather than just high assurance).
- The platform may constrain the choice of integration options.

What Other Demands and Needs Might Influence and Constrain Your Choices?

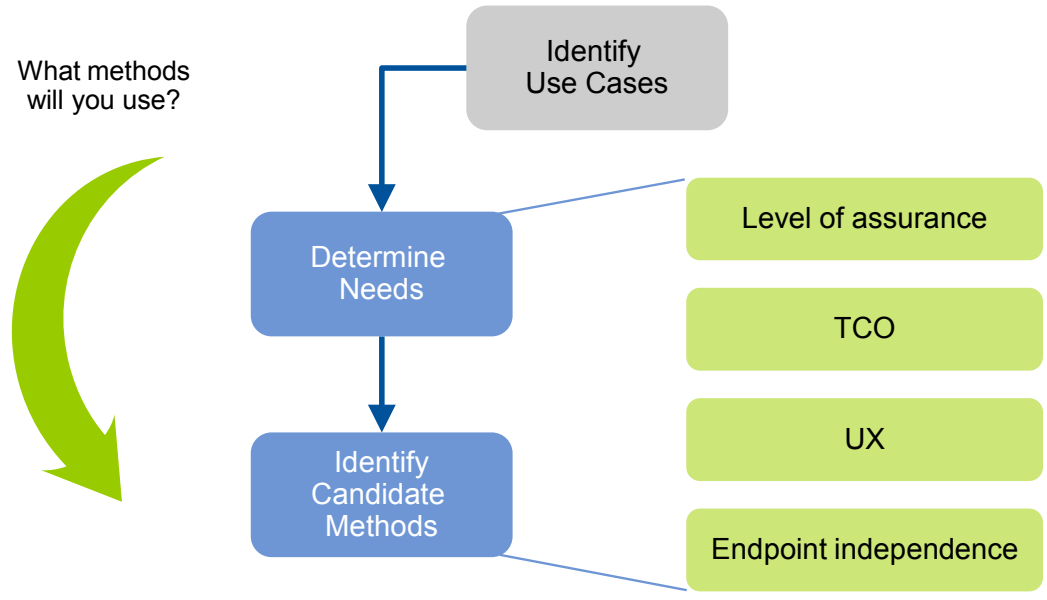
Consider these aspects:

- Laws and regulations, which may explicitly demand "two-factor authentication"
- Auditor findings, which may demand two-factor authentication anyway — even if the law or regulation doesn't[11]
- Other IT security needs — for example, a need for encryption, digital signature or transaction verification, which might exploit the same underlying mechanism as a candidate authentication method
- Other security needs — for example, a need (or desire) for common access cards.

Determine Needs and Identify Candidate Methods

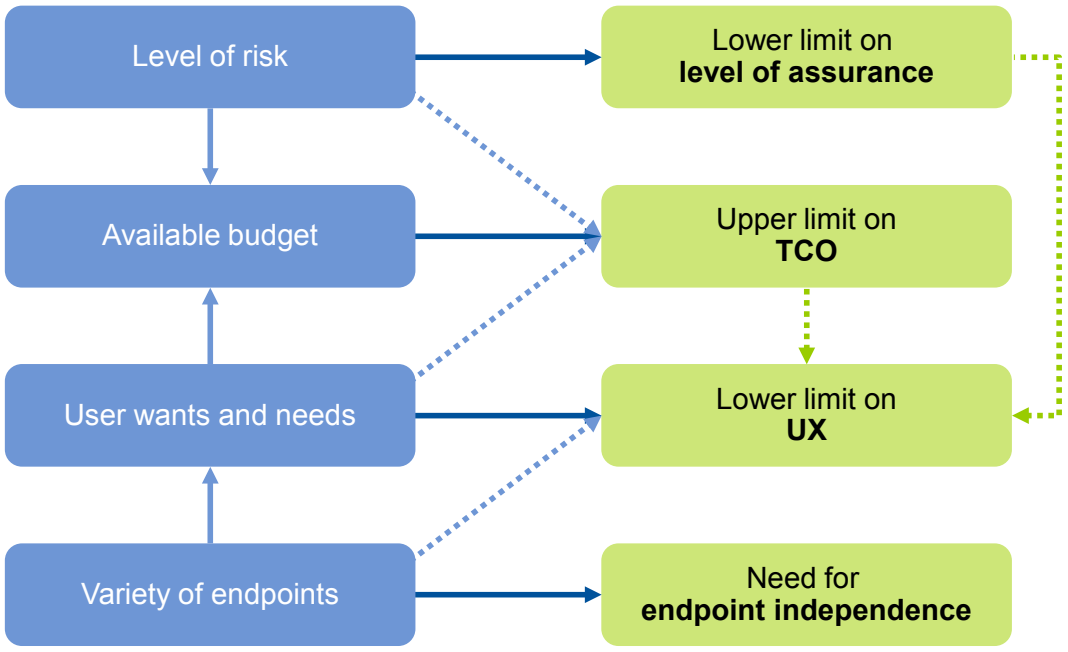
Figure 3 illustrates the scope of the first two steps in this leg.

FIGURE 3 Determining Needs and Identifying Candidate Methods



Source: Gartner (March 2013)

FIGURE 4 Determining Needs



Source: Gartner (March 2013)

Determine Needs

Figure 4 illustrates the key drivers (the characteristics of each use case) and how they influence needs.

There is a simple mapping that underlies this step:

- The level of risk imposes a lower limit on levels of assurance and accountability. Determining the level of risk in each use case is beyond the scope of this research (see "Why You Need a Risk Register").
- The available budget imposes an upper limit on TCO.
- User wants and needs impose a lower limit on UX.
- A variety of endpoints imposes a need for endpoint independence.

However, there are some dependencies between drivers:

- The level of risk and user wants and needs influences the available budget (and thus the upper limit on TCO).
- User wants and needs depend in part on the variety of endpoints (which thus determines the lower limit on UX).

Furthermore, the lower limit on UX is influenced by:

- The lower limit on levels of assurance and accountability. Since user behavior to compensate for a poor UX can create vulnerabilities that erode authentication strength, a need for stronger authentication drives good UX.
- The upper limit on TCO. As a method with a poor UX will likely have higher training and support costs, TCO constraints drive good UX.

Identify Candidate Methods

- Evaluate authentication strength. It may be appropriate to be guided by published rankings of different authentication methods, such as NIST SP 800-63-1 ("Electronic Authentication Guideline"). However, these rankings are not exhaustive in the range of methods they cover, nor is the rationale for the rankings always transparent. A "first principles" approach is presented in "Gartner Authentication Method Evaluation Scorecards, 2011: Assurance and Accountability."

In brief, this considers:

- To what degree are the authentication attributes unique, and uniquely mapped to the user?
- How hard is it for an attacker to pose as a legitimate user (a masquerade attack)?
- How hard is it for the user to willingly share authentication attributes with others?
- How do people, processes and compensating controls facilitate or mitigate an attack?

- Estimate TCO. One approach is described in "Gartner Authentication Method Evaluation Scorecards, 2011: Total Cost of Ownership." In brief, this considers:
  - Authentication infrastructure components: Hardware, software and services
  - IT operations: Implementation, support, identity administration and logistics
  - Target system components
  - End-user and endpoint components
  - Administration: Management and training
  - End users: Training and downtime
- Evaluate UX. One approach is explained in "Gartner Authentication Method Evaluation Scorecards, 2011: User Experience." In brief, this considers:
  - Learnability
  - Usability
  - Utility
  - Aesthetic appeal[12]

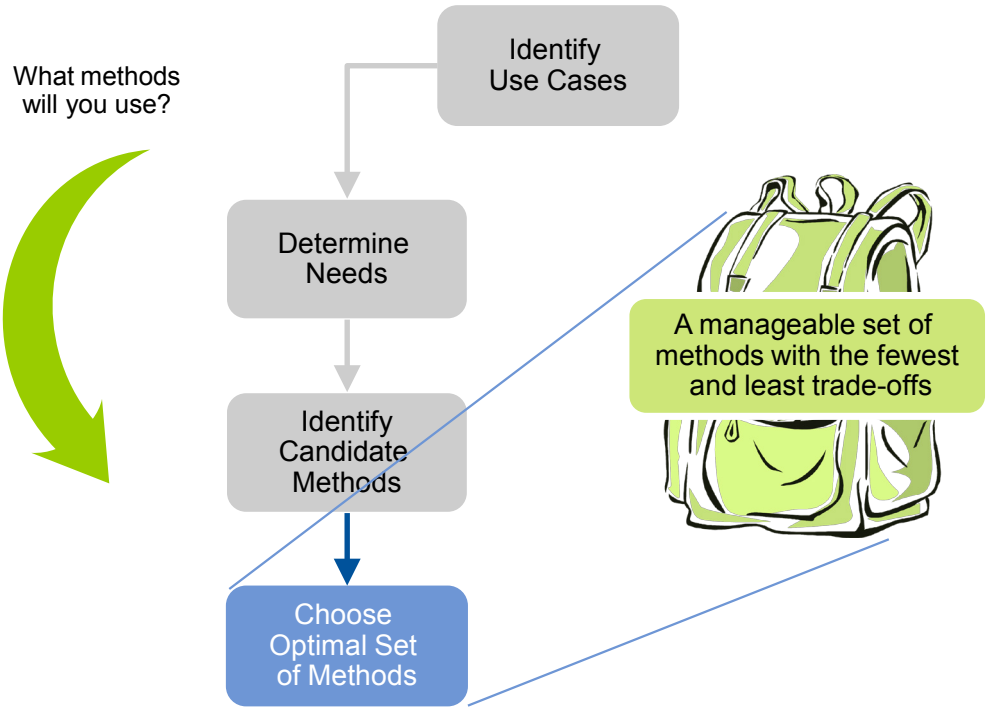
UX may also embrace privacy concerns, which are relevant to biometric and contextual authentication.

- Review endpoint independence. Consider:
  - Can the authentication method be used across multiple (kinds of) endpoints?
  - Are there differences in authentication strength among different (kinds of) endpoints?
  - Are there differences in UX among different (kinds of) endpoints?

Choose the Optimal Set of Methods

After identifying a suitable method (or a set of suitable alternatives) for each of several use cases, you need to choose the optimal set of methods from this larger set of candidate methods, as illustrated in Figure 5.

FIGURE 5 Choosing the Optimal Set of Methods



Source: Gartner (March 2013)

This is a potentially complex exercise in combinatorial optimization (essentially a "knapsack problem"). The key objective here is to minimize TCO without unacceptable compromises in authentication strength or UX.

Note that TCO is also dependent on how you will implement the optimal set of methods. In particular, having a single infrastructure that can support different methods across multiple use cases is likely less expensive than having multiple parallel infrastructures. Thus, there are dependencies between this consideration and the "How will you implement them?" leg, especially Choose Authentication Infrastructure Option(s).

The size of the optimal set will depend on the number and diversity of your use cases. Two or three is usually a reasonable target for many organizations; more than five will likely become unmanageable. A common infrastructure for multiple methods makes things more manageable and might give you the freedom to choose more methods.

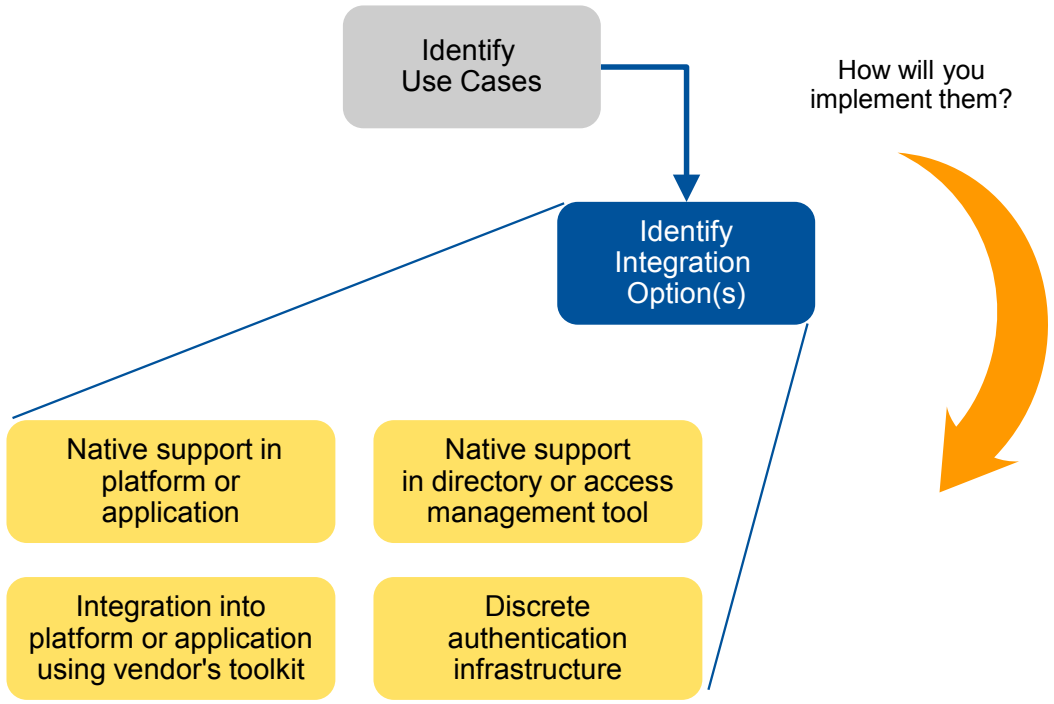
Identify Integration Options

Figure 6 illustrates the first part of the "How will you implement them?" leg.

Consider which options are technically feasible for the range of target systems in each use case:

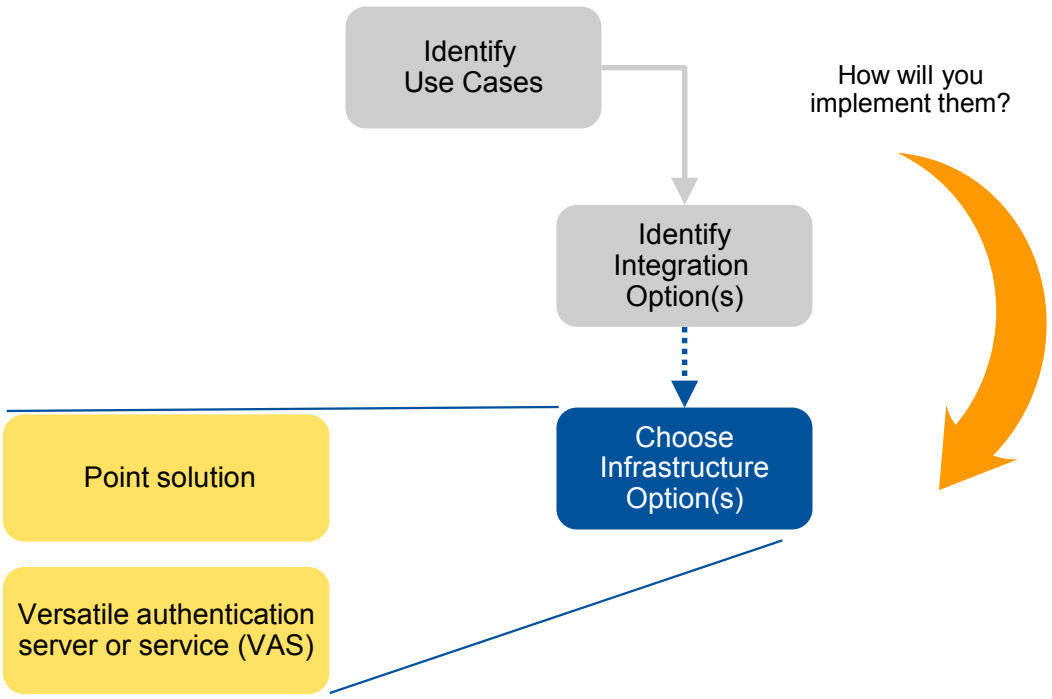
- Native support in the target system (platform or application). For example, Microsoft Windows natively supports "interactive smart card login" (that is, X.509 tokens).
- Native support in a directory (such as Active Directory) or an access management tool (such as a Web access management [WAM] tool), which can be integrated with the target system in a standard way — for example, using LDAP/PADL, Kerberos or SAML.
- Direct integration into the target system using a vendor's toolkit or APIs. This is a fairly common approach in banking applications.
- A discrete authentication infrastructure. These typically support standard protocols (such as RADIUS, LDAP and SAML) as well as providing agents, toolkits or APIs for use where target systems don't themselves support any target protocols.

FIGURE 6 Identifying Integration Options



Source: Gartner (March 2013)

FIGURE 7 Choosing Authentication Infrastructure Option(s)



Source: Gartner (March 2013)

Choose Authentication Infrastructure Option(s)

Where a discrete authentication infrastructure is indicated, the choice is between the two options illustrated in Figure 7.

A point solution describes an authentication infrastructure that supports just the vendor's own proprietary authentication methods or those integrated under an OEM agreement. A versatile authentication server or service (VAS) supports not just the vendor's own methods, but also standards-based methods (for example, Initiative for Open Authentication [OATH]-compliant one-time passwords [OTPs] and X.509), and very often has an extensible architecture to allow customers to easily integrate "any" third-party proprietary methods. A point solution might support as wide a range of out-of-the-box authentication methods, as a VAS does, but it lacks extensibility and locks-in the customer. For example, future tranches of OTP tokens must be bought from the same vendor.

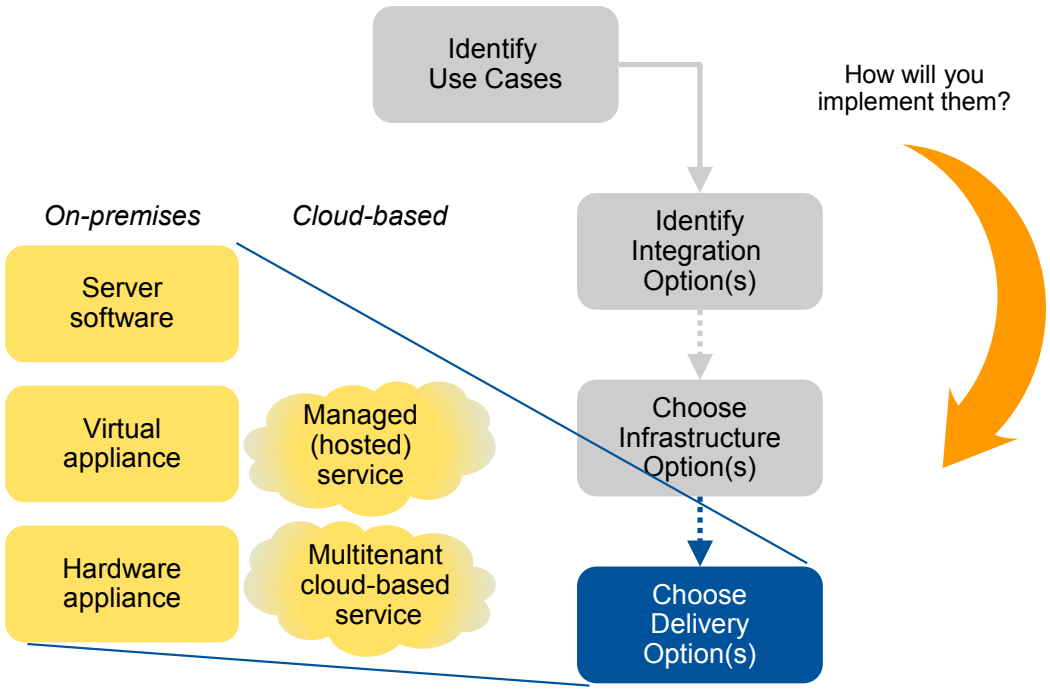
Choose Delivery Options

Whatever the chosen infrastructure option, or for each one if multiple infrastructures are necessary, choose among the options illustrated in Figure 8.

The on-premises delivery options differ in costs and support overheads (see Note 4).

Costs, resources and around-the-clock support considerations make a cloud-based service offering appealing to some enterprises, including larger enterprises in some vertical industries. Legacy managed service offerings (including those from third-party managed service providers) have typically been hosted services — that is, implemented discretely for each customer organization. Authentication vendors are now tending toward multitenant architectures, which add further simplicity and flexibility in consumption models, but which may introduce additional risks.

FIGURE 8 Choosing Delivery Options

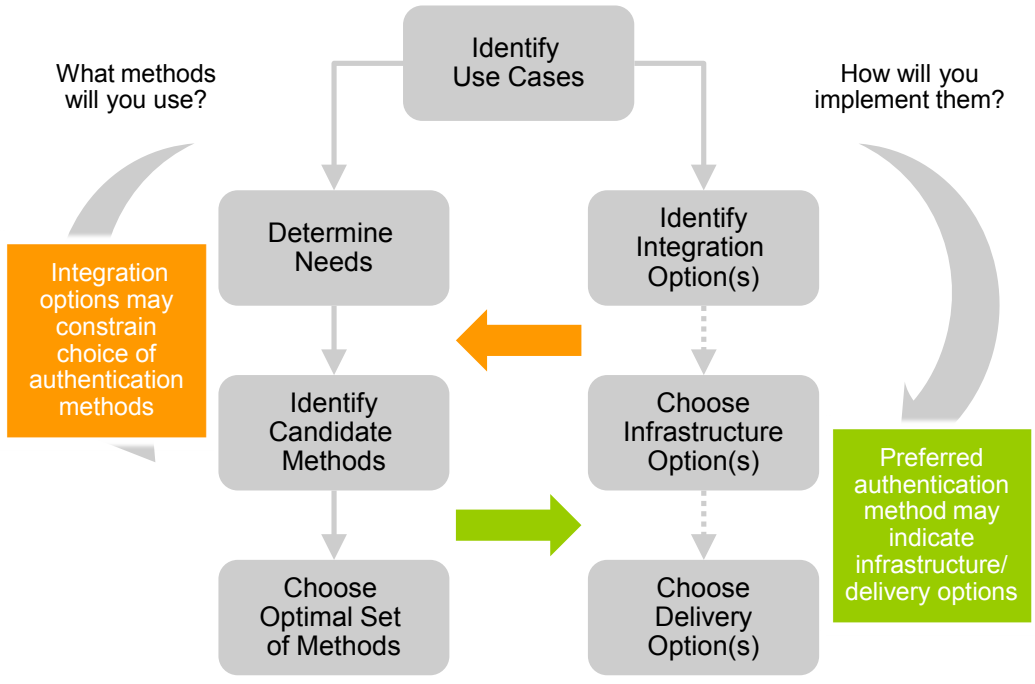


Source: Gartner (March 2013)

Review Dependencies Between Choices of Methods and Delivery Options

When you start to identify vendors that offer appropriate ranges of methods, constraints will emerge. In coming to a final decision about what methods you will use and how they'll be implemented, some iteration may be required, as the choice of methods and delivery aren't wholly independent, as illustrated in Figure 9.

FIGURE 9 Iteration



Source: Gartner (March 2013)

Evidence

[1] The 2008 Société Générale trading loss was a spectacular example of poor authentication — specifically, authentication with poor accountability — that undermined authorization and segregation of duties controls. Among other things, Jérôme Kerviel was able to use colleagues' passwords to conduct trades with their accounts. Several banks responded to this by having their traders use biometric authentication methods, which typically offer higher accountability than other methods.

[2] That is, the levels of assurance and accountability that the method provides are as high as they need to be. But they should not be higher, as that generally increases TCO or reduces UX.

[3] A person's perceptions and responses impact security and risk, TCO, corporate image and business outcomes. This is a particularly challenging issue for consumer-facing applications. In online banking, customers have actually changed banks because their old bank introduced measures that they found off-putting (see "Banks Need to Strengthen User Authentication While Appeasing Consumers").

[4] We increasingly see clients struggling to extend the use of existing authentication methods to mobile computing for a variety of reasons (see "Predicts 2013: Mobile, Social and Federation Drive Identity and Access Management"). Thus, many are choosing to use different authentication methods, multiplying support overheads and complicating things for users. This is likely to be unsustainable in the midterm to long term. As a result, enterprises should seek authentication methods that can be used consistently from any kind of endpoint — smartphone, tablet or PC.

[5] On the one hand, users who already have one or more hardware tokens are unlikely to want another. For example, we see, vendor technicians with multiple hardware tokens from different enterprise customers, and affiliated physicians with multiple hardware tokens from different healthcare delivery organizations. This is often referred to as the "necklace problem," as multiple tokens are sometimes literally fastened to a lanyard that the user wears around his or her neck. On the other hand, users who are already familiar with one kind of authentication method may prefer the consistency of using that method with multiple companies, especially if that method has good UX. For example, when people are customers of multiple banks, they may be more accepting of remote chip authentication where they can (in principle) use the same handheld card reader with each bank's payment card. Or, if they're already familiar with and comfortable using out of band (OOB) authentication, they will more readily accept it from another company.

[6] For example, a one-time password (OTP) software token on a smartphone provides a similar level of assurance to an OTP hardware token for, say, remote access to the corporate network from a user's PC. However, it provides a lower level of assurance when the user gets access to the network from the phone itself. In particular, this lack of a physical token separate from the endpoint is deprecated by some regulations and guidelines, such as OMB M-06-16 and the Drug Enforcement Administration (DEA) interim final rule on electronic prescriptions (e-Rxs) for controlled substances (see "Good Authentication Choices: Choices for Healthcare Delivery Organizations").

[7] For example, Criminal Justice Information Services (CJIS) Security Policy of 13 July 2012 allows the requirement for "advanced authentication" to be waived where users request access to Criminal Justice Information from within the perimeter of a physically secure location when certain technical security controls have been met.

[8] For example, X.509 tokens — smart cards and similar tokens — in remote access use cases can be particularly challenging: Problems with readers and PC middleware will need hands-on technical support. However, getting the PC and technician together can take days; lost or forgotten tokens can take days to reprovision, and a providing a fallback method can be technically challenging or introduce vulnerabilities that undermine the benefit of using the tokens in the first place (see "Good Authentication Choices: Evaluating X.509 Smart Tokens and Common Access Cards").

[9] We have anecdotal evidence of remote users having to step outside their houses to receive OTPs via SMS text messages and quickly step back inside to login before the OTP expires. Some vendors have work-arounds, such as "present" OTPs. Landline phones can be used for OOB authentication, although that might provide lower assurance than a personal mobile phone.

[10] This is particularly evident in regulatory requirements for authentication that are driven by certain kinds of high-value data — for example, corporate financial (Sarbanes-Oxley Act), personal financial (Federal Financial Institutions

Examination Council [FFIEC] guidance) cardholder data (the Payment Card Industry Data Security Standard [PCI DSS]), and protected health information (Health Insurance Portability and Accountability Act [HIPAA] and the Health Information Technology for Economic and Clinical Health [HITECH] Act). In some cases, the value of a physical asset managed by a system is key — for example, the DEA interim final rule for e-Rxs for controlled substances.

[11] Many regulations talk about "reasonable and appropriate" controls (this exact phrase is used in HIPAA) that leave things open to auditor interpretation, and we see that auditors tend to be conservative and go by the book (often one that was written years ago). In a sense, this may fall under the banner of risk-appropriate authentication, as it reduces the risk of audit failure while potentially exceeding the risk requirements of the application. Well-documented risk assessment and decisions about appropriateness of authentication methods are key to getting auditors to accept your choices.

[12] While this might seem irrelevant for a security technology, clients tell us that customers are sensitive to this. One European bank's customer focus group said that its remote chip authentication devices seemed "cheap and plasticky," giving a poor impression of the bank.

Note 1
Authentication Defined

Authentication is the real-time process of corroborating a claimed digital identity, yielding a specified or understood level of confidence. This definition is based on a number of similar definitions from canonical industry standards, including, for example, NIST SP 800-63-1, "Electronic Authentication Guideline."

We use "corroborating" in preference to "confirming" or "verifying" because it better conveys the idea that authentication cannot provide absolute proof of a user's claimed identity.

An alternative definition is suggested by in-progress standards work by the Organization for the Advancement of Structured Information Standards (OASIS) and the International Telecommunication Union's (ITU's) Telecommunication Standardization Sector (ITU-T) concerning "trust elevation"; that is, "increasing the strength of trust by adding factors from the same or different categories of trust elevation methods that don't have the same vulnerabilities" (OASIS, "Survey of Methods of Trust Elevation Version 1.0," 16 May 2012). From this angle, we might define authentication as the real-time process of establishing a specified or understood level of trust in a claimed digital identity.

Note 2
Types of Authentication Methods

- Knowledge — Such as enhanced passwords and grid-based one-time passwords (OTPs)
- Token — Such as phone-as-a-token methods and X.509 tokens (smart cards and so on)
- Biometric characteristic — Either a biological (physical or physiological) trait, such as fingerprint, or a behavioral trait, such as typing rhythm
- Behavior patterns — Such as browsing patterns and times of access
- Context — Nonunique identity-relevant contextual information (often aggregated)

Note that earlier Gartner research did not differentiate between behavior patterns and context, using the term "contextual authentication" to encompass both. However, behavior patterns are identified as a distinct category in in-progress standards work by OASIS and ITU-T.

Note 3
Sample Use Cases for Authentication

The following set of use cases was used as part of the vendor assessment in "Magic Quadrant for User Authentication."

Endpoint access

- PC preboot authentication: Preboot access to stand-alone or networked PC, by any user
- PC login: Access to stand-alone PC, by any user
- Mobile device login: Access to mobile device, by any user

Workforce local access

- Windows LAN: Access to Windows network, by any workforce user on the corporate network.
- Business application: Access to any individual business application(s), whether Web or legacy, by any workforce user on the corporate network.
- Cloud applications: Access to cloud apps, such as Microsoft Office 365, salesforce.com and Google Apps, by any remote or mobile workforce user.

- Server (system administrator): Access to Windows, Unix, IBM i, z/OS and other servers and databases by a system administrator (or similar user) on the corporate network. Note any restrictions by server OS or database.
- Network infrastructure (network administrator): Access to firewalls, routers, switches and so on by a network administrator (or similar user) on the corporate network.
- Other: Other system, by any workforce user on the corporate network

Workforce remote access

- VPN: Access to the corporate network via an IPsec VPN or a Secure Sockets Layer (SSL) VPN, by any remote or mobile workforce user
- Hosted virtual desktop (HVD): Access to the corporate network via a HVD thin client (e.g., Citrix), by any remote or mobile workforce user
- Business Web apps: Access to business Web applications, by any workforce user
- Portals: Access to portal applications, such as Outlook Web App (OWA) and self-service HR portals, by any remote or mobile workforce user
- Cloud apps: Access to cloud apps, such as Microsoft Office 365, salesforce.com and Google Apps, by any remote or mobile workforce user
- Other: Other system, by any remote or mobile workforce user

External user remote access

- VPN: Access to back-end applications via an IPsec VPN or an SSL VPN, by any business partner, supply chain or other external user
- HVD: Access to back-end applications via a HVD thin client (e.g., Citrix), by any business partner, supply chain or other external user
- Business Web apps: Access to business Web applications, by any business partner, supply chain or other external user
- Cloud apps: Access to cloud apps, such as salesforce.com and Google Apps, by any business partner, supply chain or other external user
- Retail customer apps: Access to customer-facing Web applications
- Other: Other system, by any remote external user

Note 4
Differences Among On-Premises Delivery Options

Server software (that is, application software meant to run on one or more server instances) may have a lower initial cost and provide the enterprise with more flexibility in how the tool is deployed, but the enterprise must provide a suitable server, harden the OS and maintain it in a secure state (via patch management), and install appropriate infrastructure protection software. Despite these issues, some enterprises prefer to supply the hardware and use their approved, supported and proven software builds.

A virtual (software) appliance (that is, a preconfigured OS and application software, typically delivered in the form of a virtual machine container) offers a plug-and-play value proposition similar to that of a hardware-based appliance, without being bundled with hardware. Many vendors use a hardened version of an open-source OS as the foundation for a virtual appliance, reducing acquisition costs. This alternative lowers the barriers to entry for vendors and the cost of adoption for IT departments. However, it is not without its own particular challenges. The organization must provide the hardware where the virtual appliance is installed. As with hardware appliances, the vendor should take responsibility for supplying patches and fixes for the entire software stack.

A hardware appliance (with preinstalled and preconfigured OS and application software) provides plug-and-play implementation. The initial cost may be higher than that of a software product, but the total cost of ownership may be lower, because an appliance may require less management. This option enables the vendor to tightly control the environment for the tool. However, the vendor should take responsibility for supplying patches and fixes, including hardware maintenance, for the entire stack. An enterprise using an appliance must also sort out responsibilities for routine tasks, such as disk capacity monitoring and log file archiving, to determine whether they will be addressed internally or performed remotely by the vendor.

Gartner RAS Core Research Note G00249403,
Ant Allan,
27 March 2013

About i-Sprint Innovations

A leading IT services provider in the Asia Pacific region, i-Sprint Innovations is the premier Identity, Credential and Access Management Solutions provider for global financial institutions and high security sensitive environments and one of the most recognized names in the financial world.

i-Sprint's security products, intellectual properties and patents exceed global financial services regulatory requirements. Organizations of all sizes benefit from i-Sprint in their administration, access control and single sign-on requirements, using an incremental, evolutionary and strategic Security Consolidation approach based on a common security infrastructure.

Established in 2000 and based in Singapore, i-Sprint has offices in Malaysia, China, Hong Kong, Taiwan, Thailand, Japan and USA and has active authorized implementation and SI partners in many countries.

Over 100 global banks, financial institutions, government agencies and large enterprises rely on their solutions to protect over USD 10 trillion of valuable assets and important information.

i-Sprint's solutions are also deployed to protect mobile devices and cloud based applications. Their dedicated R&D team has their focus on providing an integrated platform to provide authentication solutions for cloud computing, mobile devices and biometrics. Some of the successful deployments include strong authentication for Internet banking applications and single sign-on for e-Government applications.

i-Sprint Trust without Boundaries

i-Sprint's unique world leading security solutions include:

- Proven Secure E2E Encryption (E2EE) Authentication and Data Protection for convenient (Single Sign-On) and securing access to internet banking applications. Their solution meets Internet Banking Security Guidelines from regulatory agencies in multiple countries; overcoming the security challenges of most internet and mobile banking solutions.
- Bank grade versatile strong authentication (biometrics, multi-factor authentication and more) and token management platform to secure multiple application delivery environments (web, mobile and cloud) based on a common security platform.

Global Headquarters
Blk 750A Chai Chee Road
#01-01 Technopark@Chai Chee
Singapore 469001
Global: +65 6244 3900
enquiry@i-sprint.com

For a complete list of our offices:
Malaysia, China, Hong Kong, Taiwan, Thailand, Japan and United States, please visit
www.i-sprint.com