One of the most sought-after benefits from any Public Key Infrastructure (PKI) solution is non-repudiation\(^1\). Passfaces\(^\text{TM}\) support PKI in meeting this expectation. During any authenticated transaction, in addition to establishing that the identity credential presented is valid and known, it is also imperative to establish, through personal authentication, that the presenter is also the owner of the valid identity. PKI credentials alone do not provide this assurance; they only provide the link to a known identity. Passfaces\(^\text{TM}\) provide a scalable, cost-effective, cognometric\(^2\) replacement for passwords and biometrics that more reliably provide assurance of the credential owner’s presence.

Because of the increased reliability now available through the use of Passfaces, an “anonymous” authentication service can be used with a centralized credential repository to secure the online storage of users’ private keys – thus enabling the wide-scale deployment of federated Identity Management and the mobile use of PKI tokens for web services.

Public Key Infrastructure (PKI)

There are few security solutions as comprehensive in what they bring to the table as a well deployed and well managed Public Key Infrastructure. In the brick and mortar world, the trust inherent in an ink signature and in the established relationships of personal contact is essential to the business process. To duplicate that in an electronic environment requires a mechanism for establishing the non-repudiation of commitments. PKIs sell trust and bring the promise of facilitating the electronic duplication of well-established business practices.

By its very nature, an infrastructure carries with it an implied cohesion. In the case of a PKI, as with all Identity Management systems, all the security components required to initially establish the identities of a given population (identity proofing) and to make that information available and usable within a network have been designed to work together as a secure foundation in support of business applications. Time has refined the systems and their capabilities. Most of the major vendors today have had the architecture of their offerings scrutinized, evaluated, and certified for excellence.

---

1. http://csrc.nist.gov/publications/nistpubs/800-7/node239.html for definition: Non-repudiation services provide unforgeable evidence that a specific action occurred. Non-repudiation services include: non-repudiation of origin, non-repudiation of submission, and non-repudiation of delivery. Non-repudiation of origin protects against any attempt by a message originator to deny sending a message. Non-repudiation of submission protects against any attempt by an MTA to deny that a message was submitted for delivery. Non-repudiation of delivery protects against any attempt by a message recipient to deny receiving a message.

2. Cognometrics (kagnωmeutriks) n. class of personal authentication techniques based on measurable, innate cognitive abilities of the human brain (e.g. ability to recognize a familiar face).
Uses and Benefits

Once the infrastructure is in place, the PKI has the ability to support an enormous range of objectives, both security related and business related. It can provide for consistency across corporate activity, support secure inter-facility communications, and remove redundancies in building secure applications. It serves as a framework for future expanded applications and therefore a PKI’s benefits will be gleaned over a longer period than most security solutions that are less global in scope.

For many of the business benefits to be realized, the secure distribution and management of large numbers of cryptographic keys and verifiable certificates is essential. The advent of PKI as a backbone to deliver this service took large-scale secure networks out of the realm of the impossible. It allows for the secure delivery of secrets (keys) over insecure channels without a case ever being handcuffed to someone’s wrist.

For the purposes of this discourse some very explicit assumptions about the business issues being addressed by the PKI will be made. Because implementing any infrastructure, and a PKI is no exception, requires a corporate commitment to expending large amounts of capital, time, and personnel resources, the critical business needs must come from a set that justify the investment. The arguments for ROI would support that assumption. It will be assumed here, therefore, that most of the following business needs are present in some form:

- The product or services of the enterprise mandate the existence of an IT security infrastructure
- The decision has been made to utilize untrusted public networks to carry on corporate business
- There is a need to exchange cryptographic keys with partners and employees to accomplish business objectives
- There are business drivers, outside security considerations, that can be accommodated using non-reputable digital signatures.
  - Reducing Fraud
  - Conducting legally binding transactions
  - Supporting paperless contracts
  - Replacing ‘wet’ (traditional) signatures
  - Reducing liability
  - Establishing digital identities

---

3 This is supported by the Gartner article in Security Matters! entitled “PKI-What is it good for?” July 26, 2001, Note Number: AV-14-1092
When PKIs Falter

The on-going management of a PKI, whether it is installed in-house or outsourced, requires highly skilled personnel to oversee its successful operation and therefore the maintenance of its value to the business process. A cadre of security expertise, legal support, and management must be available and allocated to this complex, on-going process.

Another difficulty is the timeliness of the revocation process in a large dispersed population. This is a challenging issue when the entities served by the structure have reason to distrust each other. The revocation issue is of less importance within a trusted environment where liability is not as big an issue (e.g. Government agencies) or where other security mechanisms bind the population (e.g. DOD). When the structure of a PKI was first developed, it was envisioned that the certificate would be used off line. This was not only before on-line access was ubiquitous as it is today, but also was before on-line access to revocation lists was even available to all participants on a regular basis. Today, online access to revocation lists can be accomplished as quickly as verifying the authenticity of a certificate. More problematical may be how a revocation list can be kept current. Perhaps the day of online direct verification with the issuing CA or its proxy is getting closer.

The PKI equivalent to the Telco’s “last mile” problem is personal user authentication. The PKI itself does not tie the presence of the owner of a private key to its use in a transaction. However, any real-life implementation must address this issue if the business objectives are to be met.

User Authentication

Confusion between user identification and user authentication often occurs. Identification is the means by which a system establishes the identity of a user. Authentication is the process of establishing the validity of the identity when it is presented. A user identity code is a non-confidential and auditable representation used by the system to recognize a legitimate member of its population. The process of verifying that the identity presented belongs to the user submitting the identity code will depend on at least one of four factors:

- Something the user knows: PINS, passwords, personal information
- Something the user has: tokens, smartcards, etc.
- Something the user is: Biometrics (iris scan, fingerprints, etc.)
- Something the user can recognize: Cognometrics (Passfaces)

The goal of the process is to provide as much assurance as is necessary that the presenter of the proof of identity is the owner of the identity. Often, in order to achieve a higher level of assurance, factors are combined.
Within the context of a PKI, because user identity is core to its objectives, it is essential that great care be taken in the authentication process. Much effort and expense is undertaken initially to establish the identity of the user and to associate the user with his credentials, especially where high value transactions or legally protected information is at risk. Without high assurance that the user is present when the user’s associated identity is presented to the system, the non-repudiation of the activity that follows becomes problematical.

Proof of possession of the private key known to the system and associated by the system to the user’s identity is only part of the authentication process. A second factor is always used to establish that the presenter is in fact the owner of the identity.

The Gartner group frequently states in its reports and seminars, that they believe the ubiquity of the smartcard will facilitate more widespread use of public key-based services. Providing the user a secure trusted hardware device in which to store his private key adds credibility to his claim when he presents it to the system for use. The new Homeland Security Presidential Directive # 12, which mandates a common identification standard for all federal employees and contractors, makes the US Government a champion for this ubiquity. In the banking world, however, the high cost of issuing and managing smart cards for consumers still exceeds the expected loss from fraud. Cost is an issue in the subsequent user support and card replacement as well as in the initial deployment of any token. Another issue faced by physical hardware tokens and smartcards is that of owner responsibility. It will take time to educate persons that loss of the device, or of the secrecy of the PIN used to access it, could have potential privacy implications far in excess of the loss of a credit card. Further, if the device remains home on the dresser, its usefulness is questionable.

Biometric access to the private key holds the same elusive promise. Iris scans are considered to be as near a perfect identifier of an individual as a biometric can claim. Fingerprint scans, although still suffering from unacceptable error rates, hold similar promise as an identifier. Here again the cost of the infrastructure is significant. And too, there is the issue of privacy. Biometric images need the same safekeeping as the sensitive data they may be used to access. Precautions must be taken that the image is never stolen. Making these assurances requires strong cryptographic protocols, trusted hardware, and secure servers.

Even where the expense of hardware tokens is acceptable for a given solution, the use of a PIN or password is still the primary authenticator used to establish the presence of the token’s owner.

---

4 Gartner is a recognized source of global market knowledge for the IT and telecom industries.
Password

The community of security professionals has been predicting the end of password use for 10 years. In spite of all their faults, there are reasons why they persist:

- Intuitively, “something you know” conveys a strong sense of user presence, provided the “something known” remains secret.
- The associated cost is much lower than the hardware solutions utilizing the “something you are” proof. The cost of user education and management, estimated to run in excess of $100/user/yr, is still significantly less than the cost of anticipated hardware distribution, support, and replacement.
- Until now there has been an absence of a practical alternative. The fact that passwords are still the most popular means of authenticating the user's presence attests to the fact that scalability, cost, and usability pull hard against many multi-factor authentication solutions. Knowledge factors derive their maximum security when the known information is secret. Given the need to guard the privacy of person’s individually identifiable information, this excludes the use of information that, by its repeated use, would no longer be private like mother’s maiden name, place of birth, and social security number.

Passwords and PINS, although theoretically excellent solutions, suffer from the fact that the human ability to recall randomly generated secure strings of information is almost non-existent. Those responsible for help desk activity will attest to the fact that even user-chosen passwords are regularly forgotten. The litany of rules for producing strong passwords have not changed since their inception and yet getting compliance from a user community remains a serious challenge. Training and password strength checkers have only taught the user community how to stay one step ahead of the rules.

Another more egregious problem is the fact that users share passwords, write them down, and are susceptible to social engineering by would-be intruders. Security consultants, challenged with network intrusion tasks, are readily able to gain entry through social engineering. Most policies for resetting passwords through customer support do not adequately establish the identity of the person requesting the reset before providing the service!

Any authentication protocol based on a user secret must preserve the confidentiality of the secret. This ideally is true for the token itself as well as for the transmission and storage of the token:

- Not readily lost, stolen, forgotten, or given away by the user
- Enough entropy to assure it cannot be guessed by a counterfeit on-line user
- Protected in transit to protect against off-line attacks
- Protected in storage on both the client and server side if resident and associated with personally identifiable information.
Passfaces™

Before speaking about the synergy of Passfaces and a PKI implementation, a few words on the Passface system are in order. The Passface™ personal authentication system works by exploiting the natural human ability to recognize human faces. When Passfaces are used for user authentication, the user is presented with a series of grids each containing 9 faces: one Passface and 8 decoys. Users authenticate themselves by identifying their “passface” in each grid— a system-assigned face that they were introduced to (and familiarized with) at enrollment. A full description of the Passface System (and the opportunity to try it for yourself) can be found at http://www.realuser.com/. Further explanation is also provided as an appendix to this document.

The Passface System has important advantages over passwords:

• It is based on an innate ability to recognize a face rather than on a poor ability to recall a random alphanumeric string;

• It provides a consistent, quantifiable level of assurance. There are no “weak” Passfaces as there are weak user-chosen passwords;

• Knowledge of the user’s preferences is of no assistance when guessing their Passfaces as the Passfaces are randomly assigned;

• Unless allowed by the system, the user cannot use the same authentication secret when enrolling in other applications since the “alphabet” of faces used for any application or service can be unique (i.e. exclusive to that system);

• It provides a user secret that is easy to use and yet virtually impossible to forget;

• Passfaces cannot easily be written down or passed on inadvertently;

• The Passface™ System is completely intuitive to use and works reliably for everyone – irrespective of language, age or education;

• Help desk costs drop dramatically making Passfaces cost effective to employ.

Passfaces™ and PKI

In current PKI implementations, the authentication process is usually carried out as a two-factor process, using possession of the private key in a soft or hardware token as one factor and either
a password or a PIN as the second. This second factor is used to establish the presence of the credential owner. Passfaces offer a cognometric alternative that can more reliably establish that presence with all the scalability and low cost features of a password but without their shortcomings. This added reliability enhances non-repudiation. NIST, in its guidance for electronic authentication, SP 800-63, makes a clear distinction between the token that is used for authentication purposes and the credential that represents the identity to the system.

Locally Stored Credentials

Today, as security consciousness increases, storage of the private key on the local client has come under significant scrutiny. Reliability, as well as security, is at issue. The management of credentials stored on PCs that crash, that are susceptible to viruses and Trojan Horses, and that are easily replaced is to be considered. Even when encrypted, unless the secret used in the encryption process is remotely stored, the strength of the protection is questionable. All of these weaknesses detract from the benefits of non-repudiation that the infrastructure was built to exploit. In building a system that is forward-looking, lack of mobility also remains as another unresolved constraint in this implementation.

Alternatively, the private key could be securely stored on a trusted hardware device such as a smartcard or USB dongle, locally kept by the person whose identity it represents. For corporate applications this second device could be an appealing solution because the USB port is standard equipment on virtually all PCs sold over the last few years. Unfortunately, even if the costs of these devices drop, this solution forces the user to be responsible for carrying a device with them (and not losing it) if mobility is required. Such dongles or smartcards also require software support within browsers if they are to be used with web applications. This increases the management/installation cost and restricts mobility. Access to the credential on the device continues to be a password or pin.

In both of these scenarios Passfaces™ technology from Real User Corp produces an important improvement in the level of assurance provided by the authentication process. Passfaces™ are usually a server-based solution that offers users a usable, reliable second authentication factor as an alternative to the use of passwords. No secret information pertaining to the user is stored on the local client, only the Passface alphabet. The user can be independently verified as present through the user’s knowledge of his Passfaces, before access to the credential is granted. The entropy is consistent (no weak sets of Passfaces) and Passfaces are not easily lost, stolen, forgotten, or given away. Passfaces are user’s secrets that are system-assigned without compromising usability or the reliability sought to enhance non-repudiation.

The Real User Anonymous Authentication Service Solution

A critical factor that cannot be overlooked is the inability of the average user to understand the security issues surrounding the protection of his credential and therefore take responsibility for its care. This is a difficult issue in even the most security conscious of user communities. Users ARE a part of any system and the success of meeting the objectives for which the system was
designed, is dependent on successfully incorporating this most important fact. Today this has become even more critical because so many applications are being accessed from multiple locations such as the user’s PCs at home and at work, his PDA, and his laptop.

The value proposition here is designed to address user responsibility, manageability, mobility, and reliability as well as privacy and security. A forward-looking solution to these problems is to provide users with an online repository for their private keys – and a simple, private, and secure means to access them. This can be achieved if a PKI credential repository is used in conjunction with the Real User Anonymous Authentication service.

![Assuring User Identity & Preserving Privacy in a PKI-based Application](image)

Figure 1.

In figure 1, when a user is requested by an application to use his or her credential (1), the user will obtain his credentials by securely exchanging information with two separate servers. By presenting a token (this could be a cookie or a username) to the credential repository service (using SSL, SPEKE, or other secure protocols) (2), the repository service will securely deliver to the user the `encrypted` credential (3). Before the user can employ the credential, the user will present himself to the Passface™ authentication service. His anonymous, cognometric authentication (4) will permit him access to the key to decrypt the credential (5). By signing a token to the application, authenticated possession of the private key is revealed (6).

Much attention is being given to protocols that generate strong secrets from weak passwords\(^5\) for protection against off-line password guessing attacks. In all of this work, however, it is acknowledged that there is no implied remedy for the secrecy of the password in the hands of

---

the user. This is the contribution of Passfaces™. When protocols such as SPEKE and those proposed by Ford/Kaliski are implemented, Passfaces can be substituted for the passwords. The combination supports the mobility of today’s user while giving protection against poor user password management as well as against the feasibility of offline guessing attacks.

Key to the strategy depicted in Figure 1 is the independence of the authentication service and the centralized credential repository. Any connection between the two companies providing these services or any sharing of hardware, facilities or personnel would make possible (or at least create suspicion of) collusion. As depicted, only the legitimate owner of the credential would have temporary access to both the encrypted credential and the decryption key, thus lending credibility to claims of non-repudiation. The authentication service requires no personally identifiable information to be stored by the service. The account identifier is meaningless in the event there were a compromise of the authentication service. The account identifier is also used by the credential repository, where it is associated with the encrypted data. The anonymity provided by the separation of the authentication process from the repository of the encrypted data preserves the user’s right to privacy. The use of Passface™, the password alternative, strengthens the authentication process and increases the assurance that the owner of the credential is present during its use.

By centralizing the secure repository of the credential and by separating the authentication of the user from it, several benefits are gained:

- Authenticated access to the credential is possible from multiple locations while retaining centralized storage locations.
- The authentication can be anonymous in the sense that the service requires no personally identifiable information to be known or stored with the token.
- This same service can securely deliver, using SPEKE or SSL, the key used to decrypt the credential. Anonymity also assures this credential-encrypting key remains unusable even in the event the authentication server is compromised.
- The encrypted credential, separately stored, is delivered from the repository to the user as a separate step. Use of the credential depends on the user’s ability to decrypt it, which cannot occur until the cognometric Passface™ authentication step has transpired. This heightens the confidence that the user is present when the credential is used.
- The plaintext private key will only ever exist temporarily on the user’s own device where it will be used to sign or decrypt data on their behalf.
- Any security compromise of either the PKI credential repository or Real User’s authentication server alone would be insufficient to yield any private key to a potential attacker.
Conclusion

Personal authentication is arguably one of the most important and certainly the most fundamental of IT security requirements: all other functions in this arena (such as access control, privacy protection, data confidentiality, digital signatures, etc.) rely on the ability to confirm a person's on-line persona for their successful operation.

Even when possession of a private key on a secure token, such as a smart card, provides strong evidence of an identity, the token alone does not provide assurance that the presenter is the owner of the identity. For this a second factor is needed. Unfortunately, in practice, this personal authentication has been consistently the weakest link in the security chain. The vast majority of systems today still rely on passwords or PINs - in spite of their well-documented shortcomings. The primary reason for this continued reliance on passwords has been an absence of practical alternatives that provide scalable and cost effective solutions. Passfaces changes that.

In any PKI implementation, as with any Identity Management obligation, the greater the assurance provided by this second personal authenticator, the lower the occurrence of fraudulent access to information and applications. Passfaces currently provides higher reliability than passwords, PINS, and biometrics in establishing the electronic presence of the owner of a PKI credential during its use.

About Real User

Real User Corporation is a resident of the Chesapeake Innovation Center in Annapolis Md. Real User's Passfaces™ technology, patented worldwide, is a cognometric method of personal authentication, based on the measurement of the innate cognitive ability to recognize faces. Our products offer businesses, government agencies and OEMs a uniquely strong, reliable and cost-effective solution that can be rapidly deployed enterprise-wide to improve security and usability and generate an immediate return on investment.

For more information about the above PKI strategy, the science behind Passfaces, or the line of products, visit us at www.realuser.com or contact:

Patricia Lareau
V P Security Solutions
Tel: 805.544.1138,
Cell: 805.748.1034
pat@realuser.com
Try *Passfaces™: the unforgettable password!*