WHITE PAPER

Establishing Trust in User Identities with Strong Authentication Technologies

How to achieve the level of Identity Assurance you need, in a way that's both convenient and affordable

Executive Summary

It's a constant challenge to accommodate all the different access needs of all your users, while simultaneously locking down your resources to protect them from threats.

To trust your users are who they say they are and effectively manage their access to your resources; you need a complete identity assurance solution, the foundation of which is strong authentication.

The issuance and ongoing management, however, of user credentials, on all the various devices, from smart cards to mobile phones you need to support, for all the applications and resources your users may want to access can pose its own issues. As a result, you need a strong authentication solution that makes it easy for you to issue and manage credentials to provide differing levels of security for differing levels of access in a way that is convenient for the user – anything less negates the effectiveness of the overall solution.

The need for Strong Authentication in today's Enterprise

Users are increasingly distributed, mobile and varied, requiring many enterprises to take a new look at how to establish trust in a user's identity and control their access accordingly. In the past, most focused on perimeter defenses, putting controls in place to determine who could enter the building, with physical access systems, and who could get into the network, with firewalls and VPNs. Once inside, however, users had fairly unfettered access to all the applications and resources in these facilities and networks.

Now, recognizing the threats from users "inside their walls" – 81% of organizations have experienced a data breach as a result of negligent or malicious employees or other insiders – and watching the walls, themselves, crumble, because of the dynamic, global nature of today's businesses, many enterprises are re-evaluating their approach to access.

If you are like most enterprises, you are struggling to simultaneously accommodate all the different needs of all your different users AND minimize the risks their access can pose to your organization, which is complicated by the ever-changing threat landscape and user population. Attacks continue to evolve and become progressively sophisticated, as evidenced by the rise of advanced persistent threats (APTs) that use customized malware to conduct targeted, long-term attacks on an organization. At the same time, users, who need access to information and resources, are expanding beyond employees to include a wide variety of consultants, contractors, vendors, partners, suppliers, and customers.

All these users want to be able to access what they need from wherever they are, using whatever device they want, including their personal phones, laptops and tablets (BYOD). These variables can increase risks to your environment if you are not careful. What's needed is a way to trust the identity of all these different users and then appropriately control their access as they move throughout the organization.

Applying strong authentication to each application is one of the most effective ways you can enable the productivity your business requires, while reducing the risks to your organization. By securing the individual enterprise and cloud-based applications and data resources, whether they are on a laptop or mobile phone, you can effectively manage access and secure your informational assets.

Defining Strong Authentication to address the challenges of traditional solutions

Strong authentication, sometimes referred to as advanced authentication (AA) or two-factor authentication, goes beyond a single password to authenticate. It requires additional factors to establish the user is who they say they are. It may be something the user knows, such as a unique password or personal identification number (PIN); something the user has, such as a smart card, token, or cell phone; or even something the authentication system gathers, such as fraud and behavioral intelligence, that's used to bring the authentication to a more secure level.

Why is this important? Hackers continue to target the credentials of insiders because they give the attacker access to the facilities and network, enabling them to "look like they belong," so they can move around the organization undetected. Recent studies indicate that almost 50% of data breaches exploit stolen or weak credentials – given this stat, it's easy to see how increasing the strength of the way your users authenticate themselves can help you increase the overall security of your enterprise.

The reality is the use of traditional static passwords, while convenient, simply aren't enough to protect against today's dynamic threats – keystroke logging tools, phishing attacks, eavesdropping, and even guessing can be used to easily crack them. One-time-passwords (OTPs) and tokens offer greater security, because the password they generate is only valid for a single session or transaction, but if implemented incorrectly can create other issues. Many legacy solutions don't give you control over the token seed record, which is the "key" to that token; rather the seed records for the tokens are housed in the vendor's databases, which means a breach at that vendor could damage your company's security.

In addition, legacy solutions that assume once you're in, you're okay simply aren't comprehensive or versatile enough to consider the user's role, location and access device type to establish trust and grant access across a wide range of enterprise and cloud applications. It's not enough to use strong authentication when you first enter the building or network – as mentioned, a defensible perimeter is gone. Strong authentication needs to be extended across the organisation to include access to desktops, servers, mobile phones, data, and enterprise and cloud-based applications in a way that enables you to truly increase the overall security and accountability of your environment.

The issuance and ongoing management, however, of user credentials, on all the various devices, from smart cards to mobile phones, for all the applications and resources they may want to access can be a manual, time consuming process. It's further complicated when dealing with multiple credentials types, for physical and online access, and different credentialing and authentication systems. What's needed is a single process, with a consolidated user credential management system, that can issue and manage security credentials for all your users to grant them appropriate access to everything, from buildings to cloud-based applications, across various form factors, from smart cards to mobile phones.

ActivID Appliance versatility at-a-glance:

- **Device support:** smart phones, tablets, laptops, etc.
- **Authentication methods:** OTP hard tokens and soft tokens, smart cards, device IDs, adaptive authentication, fraud detection mechanisms, and Out-of-Band (SMS or email) OTP mechanisms for transaction level authentication
- **Applications:** Business, Cloud, etc. – such as Windows, Salesforce.com, SAP, Oracle, Google Apps, etc.

Requirements for effective Strong Authentication – no compromises

An effective strong authentication solution must be able to add security without adding significant costs or complexity. For today's enterprise environments, only an easy to use, simple to manage, strong authentication solution stands a chance to work with the wide variety of users your organisation must support to protect you against the many known and yet to be discovered attacks out there. You need a solution that provides:

Strong Authentication:

- **Two-Factor or More:** increase the confidence you have in your user's identities, so you can grant them appropriate access.
- **Differing Levels of Access:** based on the risks associated with different types of users and transactions. You should be able to deliver transparent, layered security capabilities to significantly increase your security, without impacting the user experience (at least not for users connecting from their trusted devices and locations). It can be achieved by solutions capable of doing:
- **Advanced Fraud Detection:** consider factors such as geographic location and device information when authenticating users, so you can limit access to trusted devices in trusted countries.

  Alternatively, users can be asked to use a supplementary, or more secure, method of authentication, such as a One Time Password sent over SMS, when connecting from devices or locations that are not on the trusted list.

- **On-going Behavioral Analysis:** for on-going authentication and improved forensics capabilities, using behavioral analysis of a user's interactions with applications. The user activity is constantly monitored and analysed, to learn how a specific user behaves, so that deviations from that behavior can be detected and alerted, without impacting user experience or compromising privacy.

If a deviation occurs (e.g. someone else took over the computer), the application can choose to re-authenticate the user and/or add the event to an audit database for later forensic study. This method can actually be used to reduce the number of times a user actively needs to authenticate to a system for increased user convenience.

Simplified Management:

- **Quick to Deploy and Manage**: should be easy to get the solution up and running, without adding unnecessary complexity or costs. Ideally, it would enable you to have a consolidated view to simplify the credential issuance and ongoing management of your identity assurance solutions to ensure they support your security stance (for example it should be easy to

identify and revoke credentials, so you don't have an active credential out there for an employee who has left the company).

- **Comprehensive:** single credential management system that can manage your user credentials across multiple devices, such as smart cards and mobile phones, and the ongoing lifecycle of those credentials and devices. Ideally, it would enable access to both your physical (buildings) and online assets (enterprise and cloud-based applications and resources) and provide a single, consolidated view of your overall identity assurance systems.
- **Easy to Integrate:** the solution should be able to integrate with the ongoing management tools you normally use to create a consolidated, consistent user interface for user security credentials and authentication management.

User Convenience:

- **Easy to use:** shouldn't disrupt workflows. Ideally it would leverage existing ID badges, smart cards or user mobile phones to extend secure access to the physical and online resources the user requires.
- **Seamless:** Shouldn't cause undue delay to the enterprise and cloud-based applications users need to conduct their business.

The approach for a Strong Authentication solution capable of delivering your users the secure access they need

The ActivID™ product portfolio can be used to issue and manage credentials for the wide variety of users needing access to your network, and enable them to use any device to authenticate to get the resources they need in a way that's both convenient and secure. The powerful solution consists of the ActivID converged credential, ActivID Appliance authentication server, and ActivID credential management system (CMS):

Converged Credential:

The ActivID portfolio delivers the industry's only converged credential, which can be integrated into a smart card, ID badge or even mobile phone, that can be used for both logical and physical systems to enable users to authenticate to get into a building, log onto the network, and gain secure access to the applications and other systems they need. They can also use the converged credential to gain remote access to secure networks, replacing the need for a one time password (OTP) token or key fob.

A converged credential is more convenient for users, negating the need to carry multiple devices or re-key one-time passwords. It also provides greatly improved security, by enabling strong authentication throughout the IT infrastructure on key systems, enterprise resources, and cloud-based applications, rather than just at the perimeter.

ActivID CMS Appliance at-a-glance:

You can manage your:

- **Authentication devices** – from smart cards and USB tokens to mobile phones
- **Data** – static passwords, biometrics, and demographic data
- **Applets** – one-time password applications and Personal Identity Verification [PIV] applets
- **Digital credentials** – including public key infrastructure [PKI] certificates throughout their entire life cycle

ActivID Appliance Authentication Server

The ActivID Appliance authentication server delivers the versatility you need to conveniently and cost-effectively authenticate and secure the access of your users to the applications they need to conduct business. Supporting a variety of devices and more than 15 authentication methods, you have what you need to be confident in your user's identity to grant them secure access to all your enterprise and cloud-based applications.

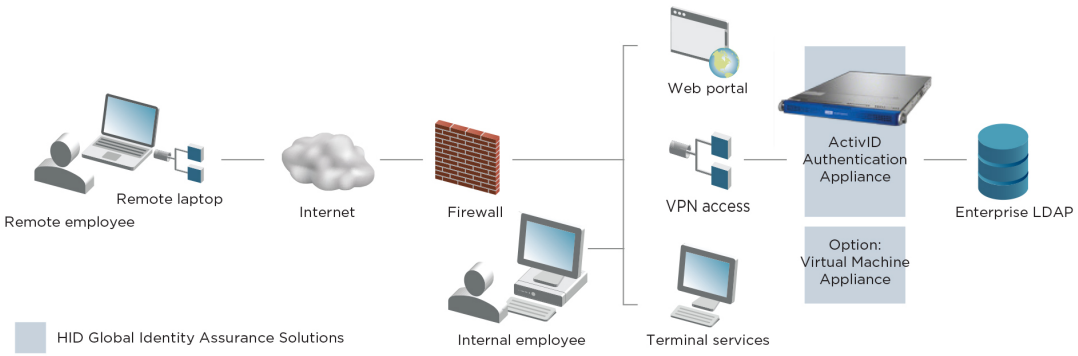
ActivID Appliance gives you the security you need, without the complexity. Templates and easy-to-define policies enable you to quickly deploy an authentication solution that matches your needs. The unique ActivID Appliance Fraud Detection Service enables you to customize the solution to meet the specific requirements of your environment. It can be used to identify access details, such as which computer users are connecting from, what browser they are using, and whether they have used it before, so you can determine whether a simple authentication is warranted or whether a two-factor should be used at that moment, based on your pre-defined rule set. This allows you to add security in a way that's simple for you and invisible to the user.

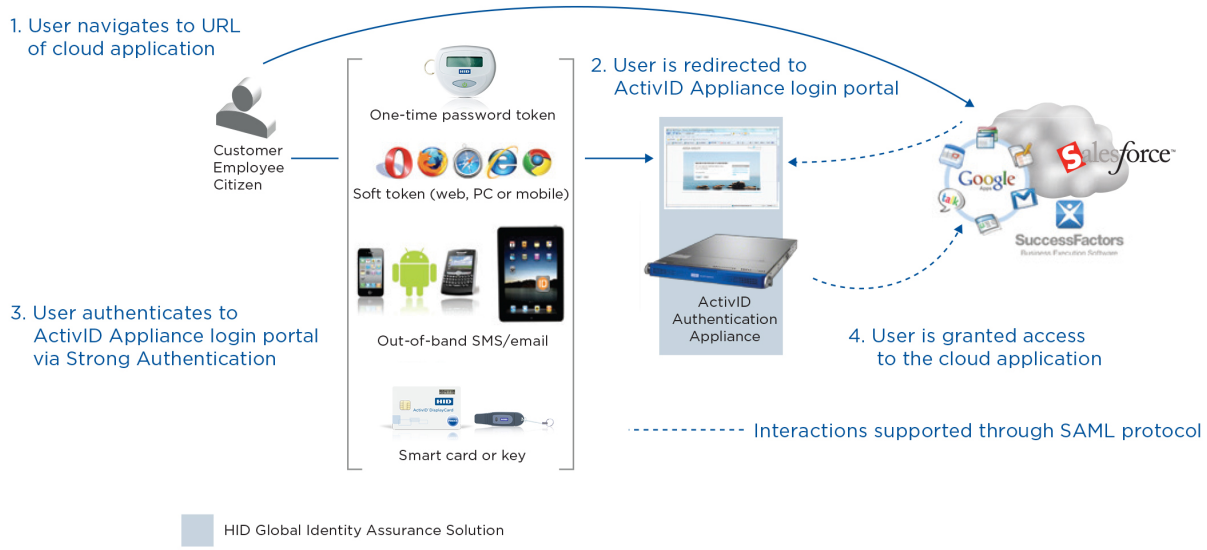
You can get as specific as you want, limiting access to particular devices within a particular area or looking at the role of the user (whether a CEO or a marketing manager, for example) and determining what credential to provision and how you want to handle their access. You can also benefit from the intelligence collected by thousands of other customers to identify whether the changing landscape (e.g. if computers from a particular area are reported to be misbehaving) should change your authentication requirements (limit access or require additional authentication.)

As a result, ActivID helps you stay ahead of your ever-changing requirements, delivering security in a way that integrates with your users' workflows to ensure you can seamlessly add protection for your critical assets. Note, the ActivID tokens last up to eight years and you can manage your own seed records to maintain full control over the protection of the cryptographic keys for added peace of mind.

HID Global Professional Services are also available to help you refine the implementation and configuration of the ActivID Appliance Threat Detection Service, should you want support. They can help you develop the best policies for your environment that take into consideration any of the more than 20 parameters at your disposal, from the role and time of day people are logging in to the location and device type, etc., to make it easy to get up and running quickly.

ActivID Appliance Authentication: How it Works

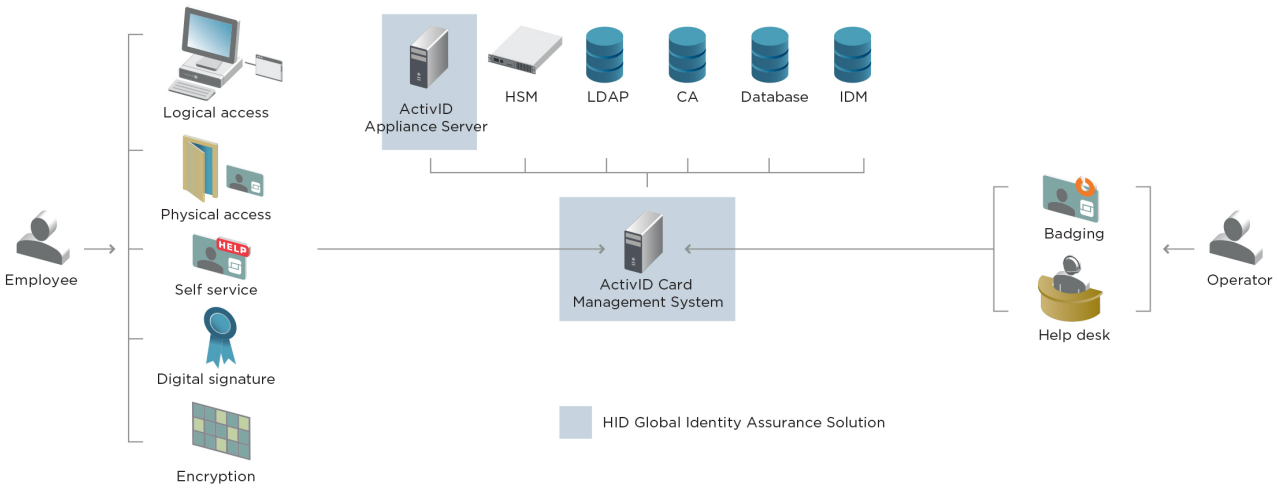




ActivID Credential Management System

The ActivID CMS provides a complete, flexible solution to enable you to easily manage the issuance and administration requirements of successful authentication deployments. You can issue and manage smart cards, smart USB tokens, and tokens on mobile phones that can be used for a wide variety of desktop, network security, and productivity applications; this enables you to set up customizable workflows and policies that readily adapt to all of your environments and deployment scenarios. It delivers full, tamper-evident audit features that log all event activities for reporting, with unique, patented post-issuance update capabilities to help you keep your authentication solution in force. Web-based self-service and help desk administration reduce the operational costs associated with the ongoing management and maintenance of the solution.

ActivID Credential Management System: How it Works



Reaping the benefits of an effective Strong Authentication solution

The complete ActivID strong authentication solution helps you increase your security, while meeting the needs of your distributed, mobile and varied users. The flexibility of the solution allows you to balance your cost and security requirements, so you can deliver the convenience your users are looking for and mitigate the risks posed by the changing threat landscape. The ActivID solution provides:

Strong Authentication:

- **Decrease risk:** securely connect users to applications via two-factor or more authentication, to inhibits breaches
- **Fraud Detection and Behavioral Analysis:** provide additional factors to consider in the authentication process to improve your confidence in your user's identity and access and make the overall user experience better.
- **Adaptive authentication strategy:** can determine differing levels of access, defining what authentication credential (device) someone needs and the type of access required by that person.

Simplified Management:

- **Quick to Deploy and Manage:** users can be quickly up and running with token authentication to secure their applications throughout the organization.
    - As the organizations needs evolve, a simple license upgrade provides organizations with access to the industry's broadest selection of authentication methods, including certificate, knowledge-based, and risk-based solutions.
    - Includes easy-to-define security policies and business processes for issuing and managing digital credentials and devices across unlimited end user groups in geographically dispersed location.
- **Reduce costs:** Single, converged credential eliminates investments in separate physical and online authentication infrastructures; simplifies processes, reduces paperwork, and streamlines the overall management of your identity assurance solution.
    - Extend the capabilities on the badge or a user's mobile phone, eliminates the need for passwords and all the processes associated with password resets, etc.
    - A versatile, multi-layered authentication platform that enables you to minimize the time and costs associated with deploying and maintaining digital identities in the form of smart cards, smart USB tokens and mobile phones.
    - Can focus your security spend on those users and applications that need it most.
- **Extend value:** a comprehensive, highly scalable and configurable management platform for multifunction employee badges, smart card-based IDs, and tokens on mobile phones.
    - Secure smartphone, iPad, laptop and PC access to VPNs, Web portals and cloud applications
    - Integrates easily with a wide variety of operating systems, directories, front- or back-end identity management and provisioning systems, certificate authorities, and physical access control systems
    - Employs fully interoperable OATH-standards-based authentication, extending the choice of authentication devices

User Convenience:

- **Easy to use:** Single ID badge or even the user's mobile phone can be used for both physical and online access; with nothing extra to carry or remember makes it easy to integrate with current workflows.

Increases productivity:

- Invisible security measures, such as fraud detection and behavioral analysis, make the solution seamless to the user and can actually reduce the number of times a user needs to authenticate.

- Policies can escalate security measures based on the level of risk and exposure to the business; this ensures any additional steps are minimized and only required when warranted (given any number of factors, such as location, device type, role, time, change in behavior, etc.)

The ActivID difference – peace of mind for users and organizations

For today's dynamic environments, only an easy to use, simple to manage, strong authentication solution can deliver on both the requirements of your users and organization. The ActivID solution gives you the flexibility you need to support and secure the wide variety of users in your organization, who are using a wide variety of devices to access a wide variety of resources and applications. It's being used by many of the most security aware organizations, from the Department of Defense (DoD) to financial and healthcare institutions. Offering the only true converged access solutions on the market, HID Global provides you the most comprehensive Identity Assurance solution, from the door reader access badge to the appliance and authentication software. Through its deployment, you can increase the trust you have in your user's identity and effectively protect your organization from the risks of today and tomorrow. As a result, you can securely connect users from any location through a variety of devices and authentication methods to help them conveniently get what they need, when they need it to confidently drive your business forward.

2014-03-20-hid-strong-authentication-wp-en PLT-01686