ehAuthenticated, civil identity credential assured online web portal access

ehAuthenticated, civil identity credential assured access to web portals and online applications

ehAuthenticated, civil & financial ID credential assured secure online banking & online purchasing

Token only and ehAuthenticated RFID access with on/off switch is optionally available

ehAuthenticated, civil identity credential assured secure online access for e-Government

Now integrated with SAML 2.0

aTrust Inc

Ottawa, ON
Canada K4P 1G1

Phone: 613-882-1114 Fax: 613-821-1706
E-mail: skhan@atrust.ca
URL: www.atrust.ca

FlickerCard™ is sold by aTrust under exclusive license from AXSionics AG.

"FlickerCard" A Personal Digital Identity Token

A FlickerCard user's physical identity & civil identity credentials can be bound to his/her FlickerCard "in person" by an authorized agent of a registration authority, an employer or a relying party.

For Web Portal Access to:

- Online e-Health
- Online Electronic Health Records
- Online e-Prescriptions
- Online Banking
- Cardless Secure Online Purchasing
- Online e-Government

In-person access to:

- eGov and eHealth facilities
- In Bank Banking
- Physical Access

The aTrust Identity and FlickerCard prevent online identity theft and protect the user against unauthorized online access in the event the user loses his/her identity by way of a lost or stolen wallet.

a-Trust —Feature Applications:

a-Mail: The Identity Service and FlickerCard are utilized in an aTrust software called a-Mail which sends and receives ehAuthenticated secure, encrypted, electronic mail and returns to the sender a "proof of delivery" message.
QTrust VPN: The Identity Service and FlickerCard create an ehAuthenticated highly secure VPN for secure remote online access to applications and data. ehAuthenticated FTP connectivity is also available.
Mimori Password Manager: The Identity Service and FlickerCard provide secure access to passwords stored online or in the case of an

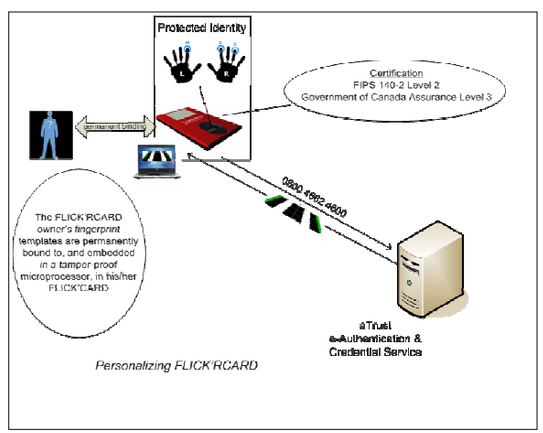
aTrust Identity Service

"Identity is Centre"

The catchphrase "Identity is Centre" was coined by Phil Becker of Digital ID Magazine. He went on to state, "By using digital identity (including biometric identity) as the key transaction and user identifier, a product or application can offer trusted computing and networking with heightened security, audited data manageability, and networking flexibilities". "If digital identity is treated as the network integrator and organizer it becomes crucial for distributed or federated tasks making recipient/sender ID, task compliance/collaboration, and task audit logs and audit trails relatively easy to compile".
Identity and electronic human authentication (ehAuthentication) should be the key offering in any credential/authentication service because identity will be verified by a credential holder many times each day, while credentials are established once and bound to the user's identity usually at the time of identity-validation and credential-proofing.
Focusing on identity-verified authentication, aTrust's user-centric FlickerCard and e-Authentication System allows the credential holder to fully control and manage his/her identity within a federated identity system or a local environment.

Online Personalization

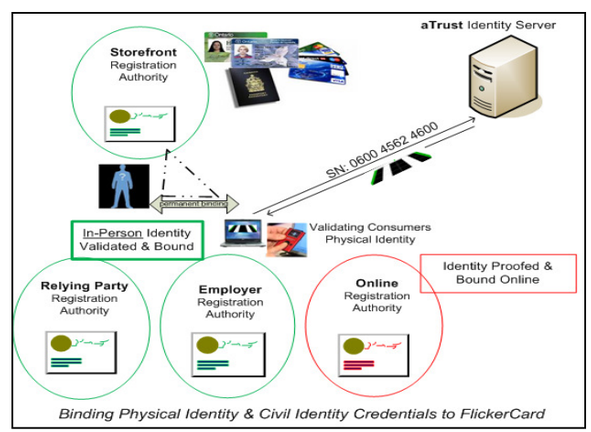
A FlickerCard owner personalizes his/her card online by registering its publicly known serial number with the aTrust Server. The Card owner also embeds his/her fingerprints into FlickerCard which are converted by FlickerCard's microprocessor into encrypted biometric templates that are stored in FlickerCard's tamper proof memory. No other personal information is stored in FlickerCard's memory.



Personalizing FLICK'RCARD

Physical Identity Validation & Civil Identity Credential Binding

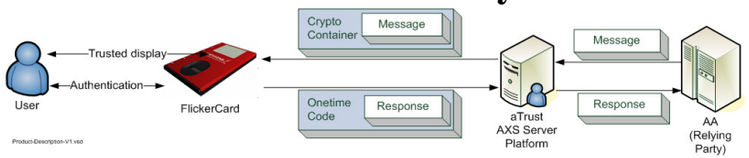
In an identity-centric environment it is important to permanently bind the biometric physical identity of an individual and the individual's civil identity credentials to a "Personal Identity Token" such as FlickerCard. Only if such a binding is firmly established, a relying party (web portal, employer, bank) will accept the identity claims of the individual.
With aTrust Identity Service we achieve this binding through a twofold process, an ehAuthenticated verification of the user's embedded fingerprint identity in the presence of a authorized agent of a Registration Authority that guarantees that only the authorized person (FlickerCard holder) is authorized to use his/her FlickerCard. The Registration Authority agent binds identity proofed credentials of the FlickerCard user to its serial number. This credential mapping of the FlickerCard user's identity assures that all future claims based on the mapped credentials are originating from the individual with the asserted identity.
Through the permanent binding of the physical identity of an individual to his/her FlickerCard, a relying party is assured that an assumption about the presented credential is valid. When a relying party accepts claims based on FlickerCard and the aTrust Identity Service the relying party can be sure the FlickerCard holder's claims are valid.
By establishing the real identity of the FlickerCard holder, the degree or level of certainty that the FlickerCard holder is in fact who he or she claims to be. The FlickerCard holder's physical identity based on the relying party's requirements is established at Authentication Assurance Levels (AL) 1-4. AL levels were established by the National Institute of Standards & Technology and are widely accepted in the US, Canada, EU, UK, Australia and many other countries.



Binding Physical Identity & Civil Identity Credentials to FlickerCard

The aTrust Federated Identity Service

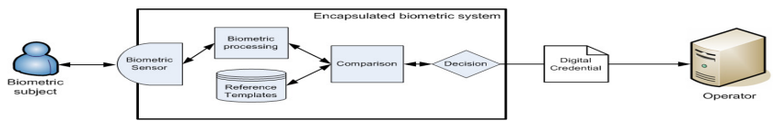
End to End Security



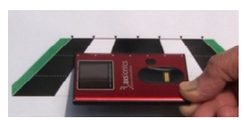
The aTrust Identity Service includes a platform over which secure end-to-end communication has been established. Each message that is sent from the web portal which is being accessed by a FlickerCard user runs over a separate secure communication channel allocated to that specific portal defining a unique and specific relationship. The communication content is enveloped in a cryptographically secure message container whose security mechanisms assure confidentiality and mutual authentication of the web portal being accessed as well as that of the FlickerCard used for the access. The freshness of the message and the correct display of the message on FlickerCard's internal secure display assure added security. The cryptographic message also contains security parameters that define one-time response codes that the user sends back to the web portal to gain access. There are protocols for different applications like one-time web portal login, financial transaction hedging, voting, transaction signing, licence checks, and recovery of a previously stored secret.

Encapsulated Biometric Identity

Millions of North Americans have no control over their biometric and sensitive personal data, which floats around in cyberspace and multiple databases. Although most people wouldn't dream of carrying around a credit card that couldn't be cancelled if it were stolen, they're giving out personal & biometric data that cannot be revoked if it's compromised. Biometrics in commercial use are non-revocable and can be "spoofed." Victims of identity theft cannot obtain a "new" set, so creating additional biometrics for an individual merely creates more opportunities for spoofing biometric data. A unique innovation of the aTrust System is the way the biometrics are embedded in FlickerCard. The storage of the biometric reference template, the measurement and the comparison process are completely integrated into FlickerCard. . The biometric data is encapsulated and protected in FlickerCard's secure (EAL4) processor memory. The biometric data, and match-on-card fingerprint processing are in full control of the FlickerCard holder and have been deemed privacy compliant by the offices of the Privacy Commissioner of Ontario and Canada.



FlickerCode is a flickering optical image. It is a cryptographic container and part of a transport layer over which the secure channel between the aTrust Authentication & Credential Server and FlickerCard is established and displayed on the user's PC monitor. FlickerCode is generated in the form of a Flash-Applet, JavaScript, or an animated GIF graphic file. It contains a one-time-password, a hedging request, and other encrypted information necessary for secure identity-verified access and secure communication.



Internal Federated Identity

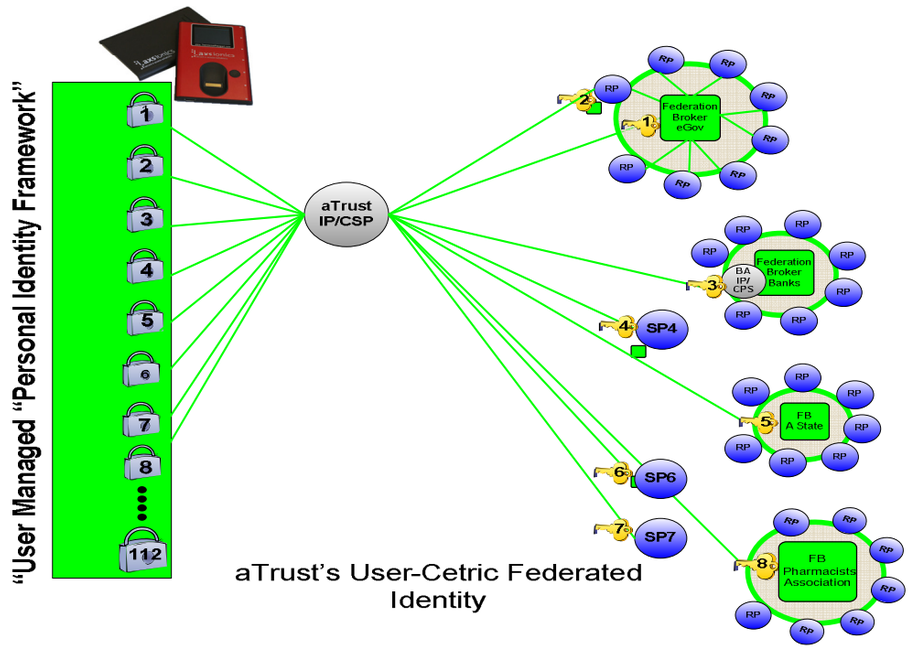
aTrust's Internal Federated Identity - The on-hand solution from aTrust involves internal federated identity and credential management systems embedded within the Identity Service software and FlickerCard. Each of FlickerCard's 112 secure AES256 bit encrypted communication channels is securely associated with a Service Provider and assures a bilateral relationship between the Consumer and the Identity Provider on one side, and with subscribing Service Providers on the other side, both sides recognizable in legal terms. Upon a user registering with a Service Provider, one secure communication channel embedded in FlickerCard is allocated to the new Service Provider and is uniquely and permanently associated and controlled by the Service Provider. However, it is the Consumer that decides whether to register with a particular Service Provider and therefore it is the Consumer that decides to let the Platform automatically allocate a secure communication channel to that particular Service Provider. This shared control of communication channels allows a flexible realization of identity federation with trust established and shared between the Consumer and a Service Provider secured by a simple bilateral use agreement. Therefore a registered Consumer gaining authorized access within an internal federated circle of trust can be recognized in legal terms by all the Service Providers in the federation because the legal, technical and business arrangements are internal to the federation and simply put in place by mutual consent.

Non-Repudiable Identity Assurance

The user's digital identity and online access rights are administered by the aTrust Identity Server. The token and relying party are first authenticated in a non-repudiable manner. Each step of the assurance process is endangered by specific threats (phishing, pharming, keystroke logging, & man-in-the middle) which compromise user authentication and target identity theft. Whereas transaction confirmation and authorization, the second part of the assurance process protects against manipulated transaction authorization. The aTrust system guards against and eliminates these threats in a *non-repudiable* manner and also provides protection against denial of service attacks.

The aTrust Value Proposition: The aTrust Identity Service and FlickerCard provide:

1. Non-repudiable electronic human authentication,
2. Non-repudiable Internet access device (FlickerCard) authentication,
3. Non-repudiable Service Provider authentication,
4. Non-repudiable transaction confirmation,
5. Non-repudiable transaction authorization,
6. Non-repudiable yes/no decision process,
7. Non-repudiable business transaction identifier as re-



User Managed Personal Identity Framework

In the scenario outlined in the diagram above, a consumer who is a FlickerCard holder with multiple mapped civil identity credentials can access, for example, a federated community of eGov, eHealth and commercial web portals. The Consumer is provided with a SAML 2.0 based electronic lock box, which can be accessed by the consumer's using his/her FlickerCard. The electronic lock box permits the consumer to grant authorized and auditable electronic access to a Service Provider with which the Consumer has registered, to encrypted security tokens containing the Consumer's confidential personal information. Through the Consumer's electronic lockbox, the Consumer can also authorize secured access to to applications containing the Consumer's private and sensitive located at different web portals to the Consumer's accountants, lawyers, employees or family members.

In the diagram above titled User Centric Federated Identity, each of the Service Providers associated with the Consumer's FlickerCard's channels 3 to 7 have a direct legal relationship with the Consumer, who were issued credentials from the Consumer's Personal Identity Framework that is embedded in the Consumer's FlickerCard. via the Identity/Credential Service Provider to the Service Providers Identity Verification Framework. In the aTrust model, Service Providers are not involved in shared or bilateral legal issues as in the legally associated federations also shown in the above diagram clustered around the Federation Broker and FB2. The aTrust Identity Service and the Consumer's FlickerCard's secure communication channels 3 to 7 have created an internal federation allowing the user to securely gain access to any one of the legally associated Service Providers. The diagram above illustrates that the aTrust model is flexible and fluid in that internally federated identities with the consent of the user migrate to a closed-loop federation and vice-versa depending on an evolving economic and legal landscape. To note, each communication channel is secured within a FlickerCard and at the Service Provider's Server by AES256 bit digital certificates.