About EtherTrust

http://www.ethertrust.com

EtherTrust is spin-off from French major research institutes (Telecom ParisTech & LIP6). It designs original and innovative security solutions based on tamper resistant devices such as smart cards, which are protected by several patents and explained in numerous technical papers. In 2009 EtherTrust was awarded by the 11th *National Contest for the Support of Innovative Start-ups* organized by the French Ministry of Research and Universities; it was also one of the finalists of *Paris Innovation Prize*.

Basis of the EtherTrust Technology

The core of EtherTrust secure platforms is based on tiny SSL/TLS stacks embedded in secure micro-controllers, referred as ***EAP-TLS tokens***. These devices perform strong mutual authentication based on certificates and asymmetric keys (RSA, ECC…), which defeat phishing attacks. The code size is about 20KB for client side and about 25KB, when both client and server facilities are supported.

The company designs multiple security components, building an efficient architecture, which provides trusted identity services for networks and WEB environments.

The following components are available:

- WEB User Agents.

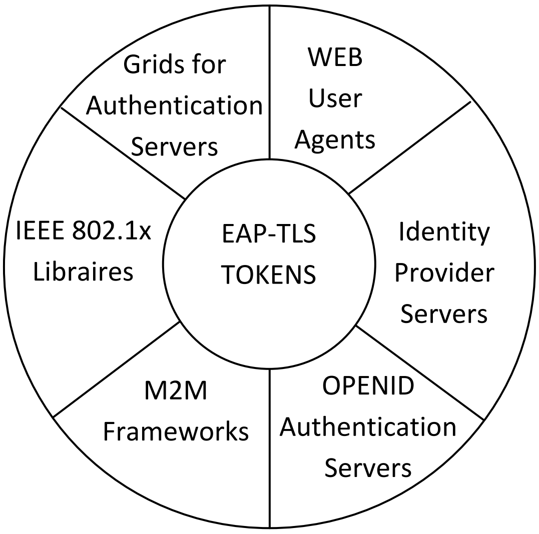
- Identity Providers Servers

- OpenID Authentication Servers

- M2M (Machine To Machine) Frameworks

- IEEE 802.1x Client Libraries

- Grids for Authentication Servers


Grids for Authentication Servers
WEB User Agents
IEEE 802.1x Libraires
EAP-TLS TOKENS
Identity Provider Servers
M2M Frameworks
OPENID Authentication Servers

Commitment to standards

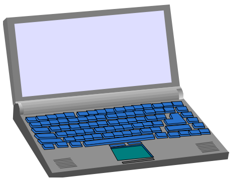
The software interface with the EtherTrust secure device is based on the EAP-TLS protocol, which is an IETF standard. More precisely information exchange is detailed by an IETF draft[1]. The internal structure of the software stack was presented during the JavaOne™ conference 2007[2] at San Francisco.

[1] http://tools.ietf.org/id/draft-urien-eap-smartcard-20.txt

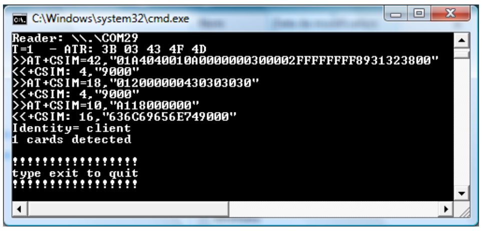
[2] http://www.ethertrust.com/resources/web/TS-0285.pdf

WEB User Agents

A Web User Agent (WUA) is the piece of software that establishes the glue between the WEB browser and the EAP-TLS token; it performs HTTPS requests, working with the embedded SSL stack. EtherTrust has developed an original and efficient technology, called ***TLS-Tandem***, providing trusted and fast HTTPS operations. These middleware are adapted to multiple contexts and use cases, targeting laptops (USB tokens equipped with smart cards), mobile phones (SSL stack in SIM cards and NFC devices), 3G dongles (including SIM cards), or cloud computing environments.



Terminal



```
C:\Windows\system32\cmd.exe
Reader: \\.\COM29
T=1  - ATR: 3B 03 43 4F 4D
>>AT+CSIM=42,"01A4040010A000000003000002FFFFFFFF8931323800"
<<+CSIM: 4,"9000"
>>AT+CSIM=18,"012000000430303030"
<<+CSIM: 4,"9000"
>>AT+CSIM=10,"A118000000"
<<+CSIM: 16,"636C69656E749000"
Identity= client
1 cards detected

!!!!!!!!!!!!!!!!!
type exit to quit
!!!!!!!!!!!!!!!!!
```

UserAgent

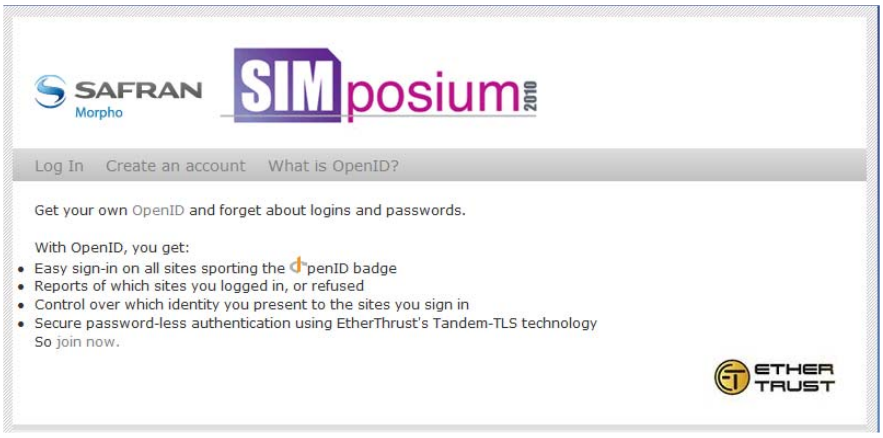
EAP-TLS Tokens

Identity Provider Servers

An Identity Provider (IdP) manages user's subscription and backup information required in case of lost or stolen token. It delivers encrypted ***Identity Container*** to EAP-TLS tokens. In the EtherTrust environment, an *Identity Container* is the set of attributes (*referred as **SSL Identity***) required by the SSL/TLS stack for proper operations. The EAP-TLS token fully manages the SSL session with the IdP server; therefore no setup is required for the terminal into which the token is plugged. In other words identity management works according to a ***plug and play*** paradigm.

OpenID Authentication Servers

OpenID is an open authentication standard supported by more than 100,000 web sites. With the EtherTrust model, net surfers are no longer required to use passwords either fix or ephemeral (OTP). Instead they are identified through SSL sessions with strong PKI mutual authentications with an OpenID server. EAP-TLS tokens are natively compatible with the WEB ecosystem because all servers support SSL & PKI infrastructure. EtherTrust devices are easily managed by a few lines of script, such as PHP with standard facilities. Optionally the OpenID authentication server may host IdP components.



Get your own OpenID and forget about logins and passwords.

With OpenID, you get:

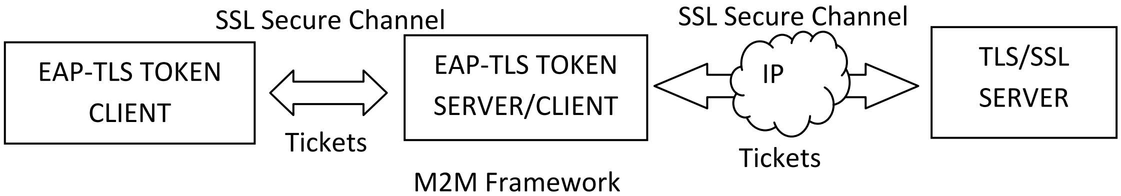
- Easy sign-in on all sites sporting the OpenID badge
- Reports of which sites you logged in, or refused
- Control over which identity you present to the sites you sign in
- Secure password-less authentication using EtherThrust's Tandem-TLS technology

So join now.

Standalone IdP and OpenID Authentication Server

M2M Frameworks

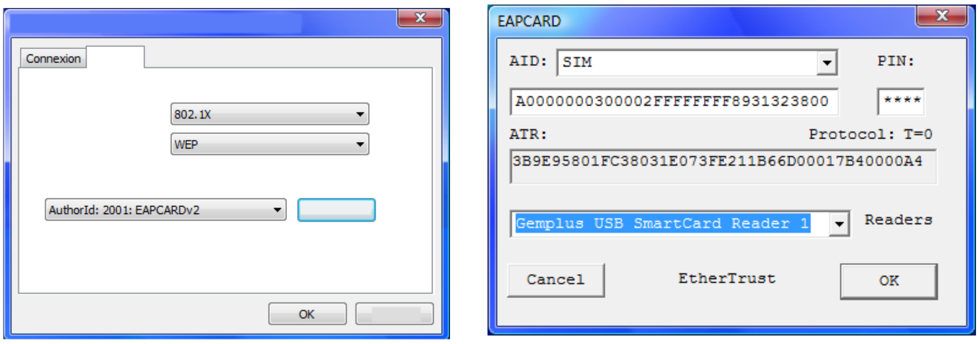
M2M (Machine to Machine) frameworks are built with EAP-TLS tokens pairs, running SSL/TLS server & client facilities, and establishing secure channels. These secure channels transport information that may be produced or store by tamper resistant devices. Prepaid applications in which tickets are exchanged between trusted entities are an illustration of such frameworks.



M2M Framework

IEEE 802.1x Client Libraries

According to the CISCO Company, most of companies plan to migrate towards ***identity oriented networks*** by 2011. The IEEE 802.1x standard was finalized in 2001; it aims at authenticating users before they can use any networks resources. It is supported by most of computing platforms including Microsoft, Linux and Apple. EAP-TLS tokens are natively adapted to this environment, and implements this standard initially proposed by Microsoft. EtherTrust has designed two libraries for WIN32 operating system called *EAP-PROVIDER* and *EAPHOST*, which work with EAP-TLS tokens for all secure login operations involving EAP (Extensible Authentication Protocol) procedures. Main usages include access control to wired (Ethernet), wireless (Wi-Fi) networks and VPN facilities.



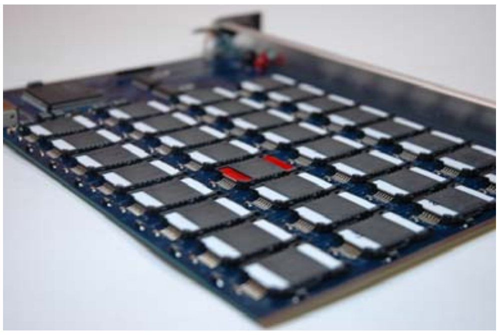
802.1X
WEP
AuthorId: 2001: EAPCARDv2

AID: SIM
PIN:
A0000000300002FFFFFFFF8931323800
****
ATR:
Protocol: T=0
3B9E95801FC38031E073FE211B66D00017B40000A4
Gemplus USB SmartCard Reader 1
Readers

EAPHOST Library for Windows

Grids for authentication servers

Identity and authentication are critical topics for all cloud services. EtherTrust is developing, with an industrial partner, grids of EAP-TLS tokens, providing SSL/TLS servers resources. A grid comprises a set of controllers, each of them managing up to 400 devices, split in 32 units per electronic boards. As an illustration a RADIUS server is divided in two logical blocs, a pure software entity and a grid of trusted SSL servers. Thanks to this innovative architecture companies may externalize they authentication infrastructure, with a high level of security.



Grids of EAP-TLS tokens