



■ TECHNOLOGY ■ CONSULTING ■ INNOVATION

ELCA

WHAT IS **ELCARD** ?

A Strong Authentication Solution for Large Public Deployments

SIMPLE • CONVENIENT • SECURE • LOW COST • RELIABLE • FLEXIBLE



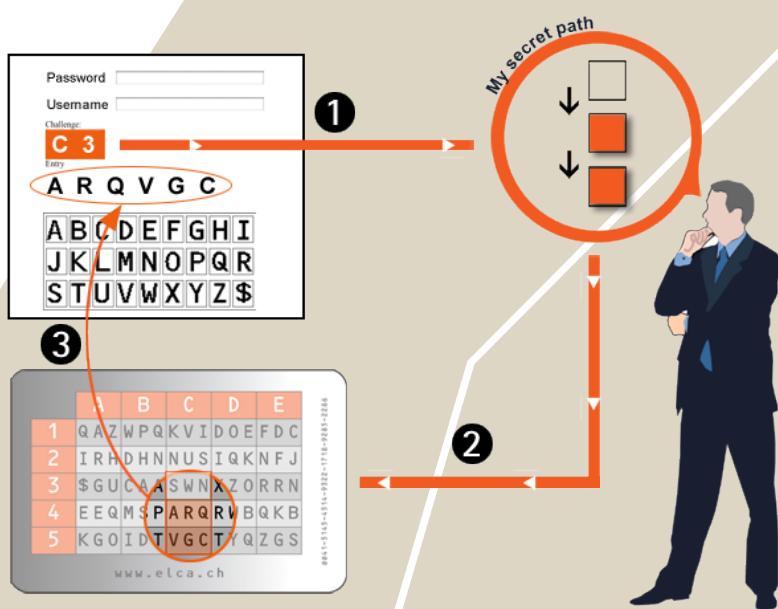
«Strong Authentication for Large Public Deployments»



The need for strong authentication on the Internet is becoming even more urgent and "phishing" attacks to pinch private passwords are rapidly increasing. Meanwhile, though, existing protection alternatives are much too expensive and not really suited for a large public deployment. Users are not ready for electronic tokens that they don't understand or trust—and they don't want to shoulder high costs or wait days for a replacement. ELCARD is an innovative approach that relies on inexpensive non-electronic cards and a robust set of self-service utilities to satisfy user requirements—without any security trade-offs.

ELCA

A card is **simple, convenient and secure**. Users are comfortable with the form factor, intuitively understand "how it works", and do not hesitate to carry cards around.



SIMPLE

Users answer a one-time challenge with a personal one-time response from the card in order to prove their identity. They simply use their card like a bingo card or naval battle grid:

- 1) From the **challenge**, users spot the cell intersecting the corresponding column and row. For example, <C3> in the figure to the left relates to the cell in column C and row 3.
- 2) Users then read the content of adjacent cells along a **personal and secret path**. In the figure to the left, with the path being <DOWN, DOWN>, the user reads ARQ and VGC.
- 3) Finally, users enter the required symbols one by one, using mouse clicks on a **virtual keyboard**. The answer in the figure to the left is, then, <ARQVGC>.

(Try it with the challenge <D1> and a path <DOWN, RIGHT>. If you find <IQKNFJ>, you are now trained on ELCARD !)

If a user has forgotten his secret path, ELCARD provides self-recovery mechanisms to allow him to confidentially retrieve it.

CONVENIENT

There is no limit to the supported symbol sets for challenges and answers – and the virtual keyboard displays exactly the same symbols as the cards. This eliminates potential user confusion, for example, between '0' and 'O', or between 'l', '1' and 'L'. There is no problem with internationalization, either!

Cards may vary in terms of format, security, usability and layout. Cards can be customized to suit every level of user sophistication and users may be allowed to select the card they want.



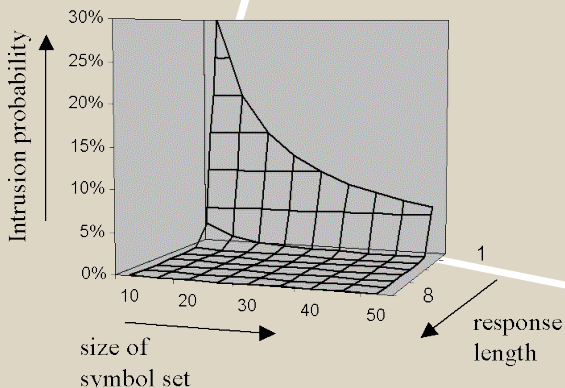
SECURE

Depending on the configuration of cards, there can be billions of possible answers to a given challenge. The number of attempts is limited through system configuration and a new challenge is generated after each attempt. After too many failed attempts (e.g. 3), a card will be locked by ELCARD.

ELCARD provides a real, self-contained, **2-factor authentication** capability. Users combine their card (what they have) and their secret path (what they know). If someone steals the card, its use remains protected by the secret path.

Using ELCARD **on-line services**, users may lock their card, suspend use during a vacation, and request a new card. They may also, without Helpdesk involvement, unlock their card and modify their secret path.

ELCARD informs users about the status of their card and recent authentication attempts. Victims of suspicious events may be systematically notified and requested to lock their card, request a replacement, ...

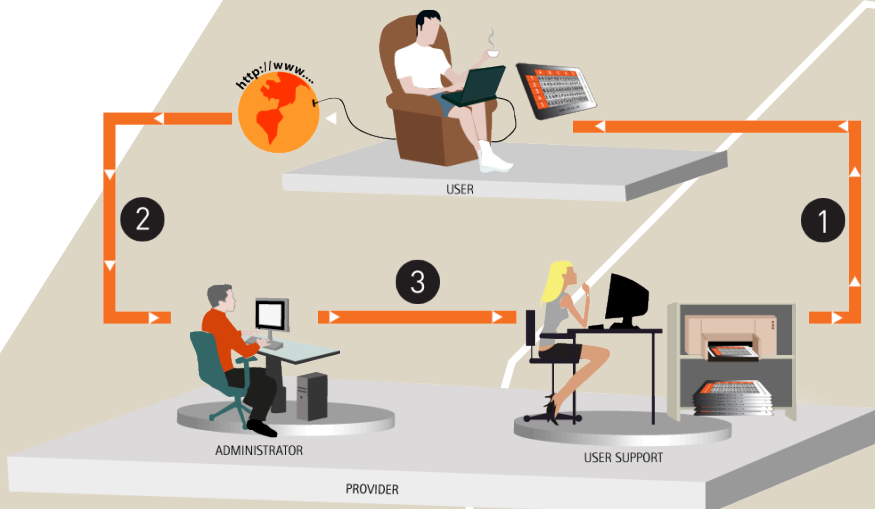


«Strong Authentication for Large Public Deployments»



Existing solutions for strong authentication have proven their suitability for limited deployments inside the enterprise, where the environment is under control, the number of users remains reasonable and the return on investment is obvious. This is different on the Internet. The size, and diversity of the audience, the distance and local specificities, as well as the complexity and volatility of services make these solutions very expensive and complex. ELCARD is a software solution focused on providing a satisfying response to the Internet authentication challenge while significantly reducing the total cost of ownership.

ELCARD is a **low-cost, reliable and flexible** software solution that fits in with your existing processes, services, budgets and IT infrastructure.



- With ELCARD, the provider has the full solution to:
- 1) Produce the cards and send them to the users with the necessary info
 - 2) Monitor the activity and process pending requests from users
 - 3) Retrieve the runtime info for distribution and the distribution lists

LOW COST

The production of laminated or printed cards can be accomplished via existing **office printers or card production facilities**. Cards can also be e-deployed.

There is no need to associate cards with users before sending the cards out. Users securely perform the registration themselves when they receive their card.

The number of cards that can be produced is unlimited. Replacement cost is limited to materials, printing and shipment. Simple periodic refreshment of the secret path extends the life of a given card almost indefinitely.

Thanks to the extensive set of on-line utilities provided with ELCARD, support to users is reduced to an absolute minimum so helpdesks can focus only on truly exceptional cases.

ELCARD allows administrators to process cards one by one or in batches. Therefore, monitoring 1,000 registered cards doesn't take any more hands-on time than 1,000,000.

RELIABLE

ELCARD incorporates the **architectural standards** recommended and widely accepted by the web and security markets.

- Best-of-breed security algorithms and mechanisms protect the system against both internal and external attacks
- Redundant deployment on multiple machines guarantees high performance and high availability of the service

Even when deployed on a single basic server, ELCARD is capable of high performance—handling up to 10 parallel authentications per second with an average response time below one second.

FLEXIBLE

Integrating ELCARD with on-line services is straightforward and requires either:

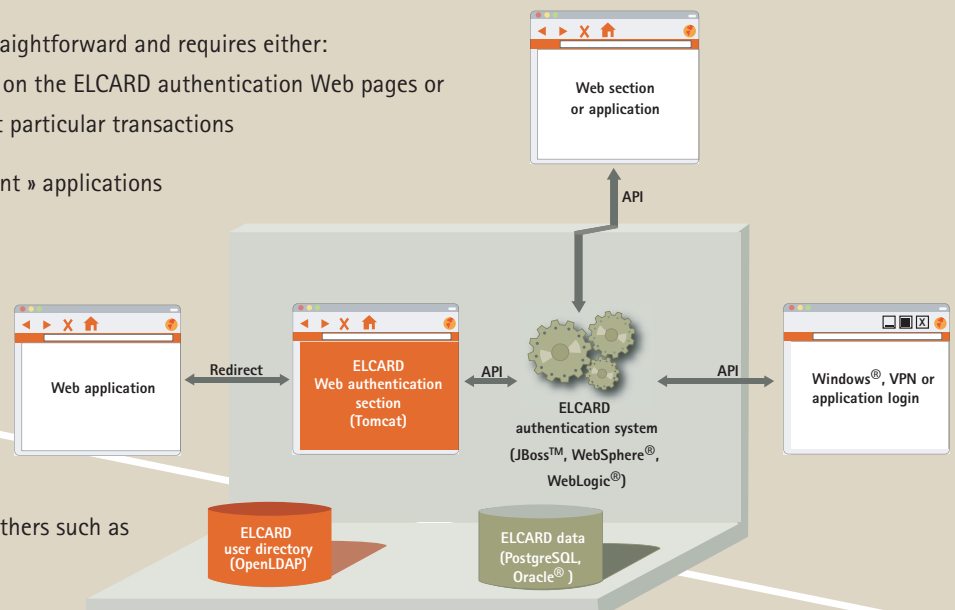
- Redirection of non-authenticated sessions on the ELCARD authentication Web pages or
- Calls to the ELCARD API in order to protect particular transactions

Integration alternatives: Windows®, « rich client » applications and VPN clients.

Alternative distribution media for cards and information: email, fax, MMS, voice mail, Web, ...

ELCARD is supported on the leading software platforms and their open source counterparts:

- Application servers: JBoss™, Websphere® and Weblogic®
- Databases: PostgreSQL and Oracle®, and others such as MS SQLServer® or MySQL on demand



A Strong Authentication Solution by



■ TECHNOLOGY ■ CONSULTING ■ INNOVATION

ELCA

IT-Solutions by ELCA. We make it work

ELCA, Av. de la Harpe 22-24, case postale 519, 1001 Lausanne, Suisse
Tél. +41 (0)21 613 21 11, Fax +41 (0)21 613 21 00, info@elca.ch, www.elca.ch

