Latch

THE ALTERNATIVE TO GRID CARD

Grid Card: a death foretold

Today banking entities providing products and services on the internet use different authentication techniques to identify their clients. Single-factor authentication models have fallen behind, giving way to strong authentication processes that require a combination at least two elements, categorized as:

1. Knowledge: *Something that the user knows such as a password or PIN code*
2. Possession: *Something that the user has such as a token, smartcard or cell phone/SIM*
3. Inherence: *Something that the user is, a biometric characteristic such as a digital fingerprint*

The banking sector normally employs a risk-based authentication model, generally using two levels to permit access to their online services:

Banking sector authentication levels for accessing online services	Common authentication methods	SOMETHING YOU KNOW	SOMETHING YOU HAVE	SOMETHING YOU ARE
The **first authentication level** enables access to basic online banking services such as checking balance, transactions or the status of contracted services	Username – Password	■		
	Digital certificate	■	■	
	eID	■	■	
The **second authentication level** generally applies to the validation of operations (authorization) that entail a certain risk such as economic transactions or personal data modification. There is normally an assumed deterioration in usability in exchange for greater security	Grid card		■	
	OTP - disconnected tokens		■	
	OTP - sms		■	
	OTP - soft token		■	
	eID	■	■	

Deadline

The strong authentication concept had no official definition until January 2013, when the European Forum on the Security of Retail Payments (SecuRe Pay) published a comprehensive guide with recommendations for fighting and preventing payment fraud on payment service providers, that, among other things, defined the minimum criteria that a strong authentication process should fulfill, and whose implementation must be completed by 1 February 2015 as per the indications of the European Central Bank.

JANUARY 2013
SECUREPAY RELEASES A COMPREHENSIVE SET OF RECOMMENDATIONS TO IMPROVE THE SECURITY OF INTERNET PAYMENTS AND PREVENT FRAUD

Strong authentication definition is set

ACCOMPLISH WITH THE ECB CRITERIA FOR STRONG AUTHENTICATION PROCESS IS A MUST

WHO IS AFFECTED?
Applicable to governance authorities of payment schemes and all payment service providers (PSPs) that provide internet payment services

WHERE APPLIES?
EU28 and SEPA zone, Switzerland, Norway, Liechtenstein, Iceland and Monaco

FEBRUARY 2015

DEADLINE FOR IMPLEMENTING THE RECOMMENDATIONS

The Grid Card is obsolete

The European Central Bank has underscored a need in that the initiation of internet payments, as well as access to payment data, should be protected by strong authentication. Let's examine whether most common mechanisms implemented by banks and payment methods meet the minimum established criteria:

	Applied Authentication Process *First authentication level (login/pass) + 2FA*				
Minimum criteria	*Grid Card*	*OTP (sms)*	*OTP (software)*	*OTP disconn. Token (HW)*	*eID*
*The authentication process uses **two or more elements** to prove the authenticity of the user*	✔	✔	✔	✔	✔
*Independent third parties have **certified/assessed** that the security level of the devices is robust and tamper-resistant*	✖	✔ Infraestructure ✖ Mobile device	✔	✔ SIM-based solutions	✔
*The security mechanisms follow **publicly available and recognized standards***	✖	✔	✔	✔	✔
*The payment process is initiated via a **independent channel***	✔	✔	✔	✔	✔
***Non-propagation:** The violation of one of the authentication elements does not affect the protection for the rest*	✔	✔	✔	✔	NA
***Non-reusable:** authentication codes are non-replicable, since they are accepted only once by the system*	✖	✔	✔	✔	NA
***Non-replicable:** it is not feasible to clone and secure an exploitable copy of the element, or to steal confidential information via the internet*	✖	✔	✔	✔	✔
***Confidentiality** is guaranteed from the moment authentication is initiated to its verification by the server*	✖	✖	✔	✔	✔

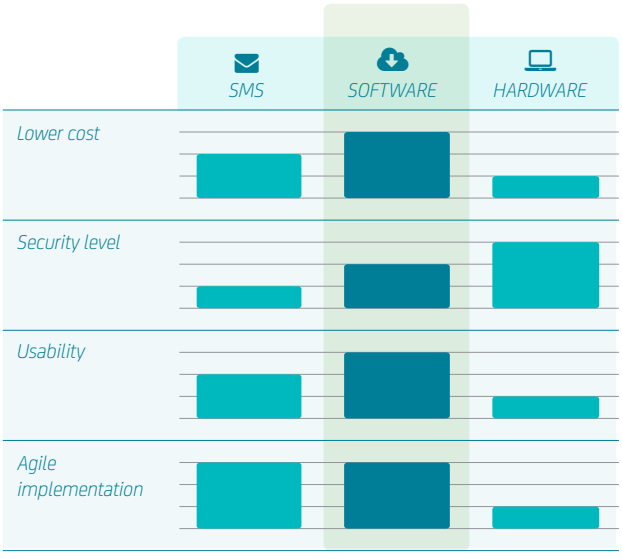
From the comparative above, we could conclude that the grid card has become obsolete as a user authentication element, yet it is one of the most common practices in online banking. In light of the indications given by the European Central Bank in this regard, Financial Entities currently working with grid cards should progress to other models.
Which is the best alternative in this case?

The best alternative: OTP software

Among the different OTP solutions, token software has the best cost-benefit ratio:

- **Fulfills** ECB indications
- **Reduces costs**, eliminating SMS payments or the need for HW purchases (tokens) and their maintenance
- Insofar as its **usability**, it benefits from the generalization of internet-linked smartphone usage
- **Accelerates the implementation** by eliminating the need to deploy physical elements (tokens and infrastructure)
- Offers better **security** characteristics compared with SMS in view of cryptographic implementation and possible use of secure smartphone containers

One Time Password



Latch as an alternative to grid cards

Continuing with the analysis, and now focused on OTP software as the best alternative to replace grid cards, the following question to address is: which OTP software solution to select?

To respond to this question, we propose a comparative study of the different types of OTP software solutions with the considerations that the ECB identified as key when establishing strong authentication mechanisms:

Key consideration	*OTP GENERATED REMOTELY AND SENT VIA EMAIL TO THE USER*	*OTP GENERATED ON THE MOBILE DEVICE THROUGH AN APPLICATION*	*OTP GENERATED REMOTELY AND SENT VIA PUSH NOTIFICATION TO THE MOBILE APPLICATION*	Latch PROTECTED
Protect the initiation of internet payment and access to private information with strong authentication	■	■	■	*a*
Establish transaction monitoring mechanisms conceived to prevent, detect and block fraud				*b*
Limit the number of authentication attempts and define time-based rules for sessions and authentication validity		■	■	*c*
Implement multiple defense layers at the security level to mitigate risks				*d*
Provide assistance and guidance to users regarding best online security practices, offering them alert tools and transaction tracking features				*e*

Latch meets ECB key recommendations

In addition to a second factor of token-push authentication, Latch clearly enriches the security by engaging on the main considerations underscored as key by the ECB:

A) Latch as strong authentication

Latch not only limits the exposure of authentication processes, but also protects the initiation of any critical process with strong authentication because of the Latch-incorporated second authentication factor (token software).

This token is generated by the Latch service and sent over SSL to the user application and bank (or financial entity) through an independent channel (out-of-band).

The user receives the token through the mobile app (token push), will be defined by the Bank (for instance, 60 seconds).

B) Latch for early detection

Financial entities and payment service providers have been pioneers in the use of fraud detection tools, working to identify fraudulent patterns and examine context to identify risks.

Nonetheless, the incorporation of Latch as an ancillary element to these systems affords a unique perspective for early detection in cases of identity scams following the theft and usage of credentials:

- **Detection:** the user will be alerted through the mobile application in the authentication/authorization process in which the Bank has implemented Latch, whether the user has initiated the process or a third party in an impersonation attempt.
- **Prevention:** Latch enables users to block their digital accounts when they are not being used, thus preventing unauthorized use.
- **Blocking**: the mobile application will notify users of any attempt to access banking systems with their identity, thus enabling the bank to engage a temporary block for cases in which there is a fraudulent use of its users' credentials.

C) Latch for establishing time limits to the authentication validity

The Latch service also has the option to establish time limits on the authorization process, for instance, by programming automatic blocking for certain operations after a given amount of time has elapsed since access or fixing an hourly time window (e.g., at night).

D) Latch for multiple layer protection

The philosophy behind Latch is simple: if we keep our accounts or digital services blocked while we are not using them, we reduce the risk of their fraudulent or unauthorized use. For instance, we could block the initiation of an online banking session, credit card payments or the bank transfer authorization process (any transaction over which we want to apply this control).

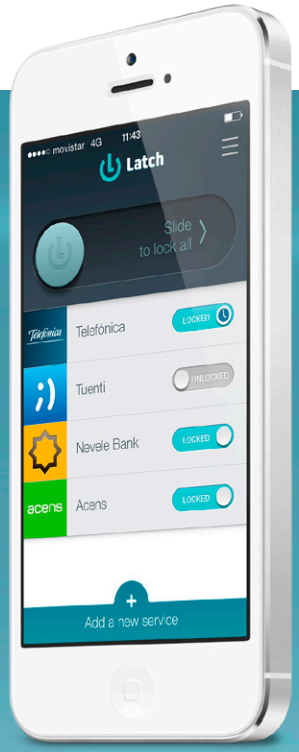
Latch thus provides an additional layer to buttress overall security, thus reducing the exposure time of operations:

- It is not an alternative to banking's current authorization processes and systems and it is fully independent of the authentication arrangements that this sector uses.
- No bank user information is required: Latch APIs and SDKs are employed during the user authentication process to check the current status of the user's account but no information is exchanged regarding the service user.

E) Latch as a tool offering users control over their security

Providing users with control over their services (payments via credit cards or bank transfers) affords a clear improvement in their perception of security:

- Latch will inform users of access attempts using their digital identity.
- Users may define the availability of their own services, e.g., by indicating certain time slots (such as nighttime) to block access.



Benefits of Latch
as an alternative to grid cards

Replacing grid cards with Latch tokens renders the following benefits:

- ✔ **LEGISLATIVE COMPLIANCE:** Strong authentication model that fulfills the new ECB regulations.
- ✔ **CONTROL OVER EXPENSES:** No infrastructure investments and cost control from the very outset (licensing for active users).
- ✔ **AWARENESS:** Improving user experience while getting them involved in their security.
- ✔ **ADDITIONAL SECURITY:** In addition to strong authentication, Latch provides an additional security layer, agile monitoring and user involvement in controlling their own security.
- ✔ **ON SCHEDULE:** Quick and easy implementation meeting the deadline of 15 February 2015.

Eleven Paths

More information at:
elevenpaths@elevenpaths.com
Latch.elevepaths.com
elevenpaths.com
@ElevenPaths

A Telefónica COMPANY