Visible Digital Seal

&

Otentik Trust Network

Or the story of a small object locked in a cage

Gilles Barré

Visible Digital Seal International Council

2D-OK

Everyone knows the cage,

and therefore believes he knows this object…

…without opening the cage!

The object is the Visible Digital Seal (VDS),

The cage is its representation in the form of a 2D code,

The infrastructure is the OTENTIK trusted network.

Vidéo : OTENTIK Trust Network presentation

https://otentik.codes/ressources/

https://www.youtube.com/watch?v=71d6Dxo1Z_w


THE OTENTIK TRUST NETWORK

OTENTIK VDSIC

tuntrust
Agence Nationale de Certification Electronique

The VDS is a variation of the electronic signature.

Unlike the electronic signature the VDS secures the key data of a document and not the entire document

Federation and administration of existing trusted environments to achieve interoperability of VDS is needed

This is the purpose of the Visible Digital Seal International Council that we created in 2016.

As the circulation of documents (or objects) is global, fraud is also global.

In order to effectively combat this scourge, our objective is to develop an international network of trust, based on an interoperable and non-proprietary solution.

To achieve this objectif :

a) **We have standardized the VDS in France (AFNOR XP Z42-101 & -104)**

We will continue the work of standardization at the international level by creating the conditions for simplifying its use.

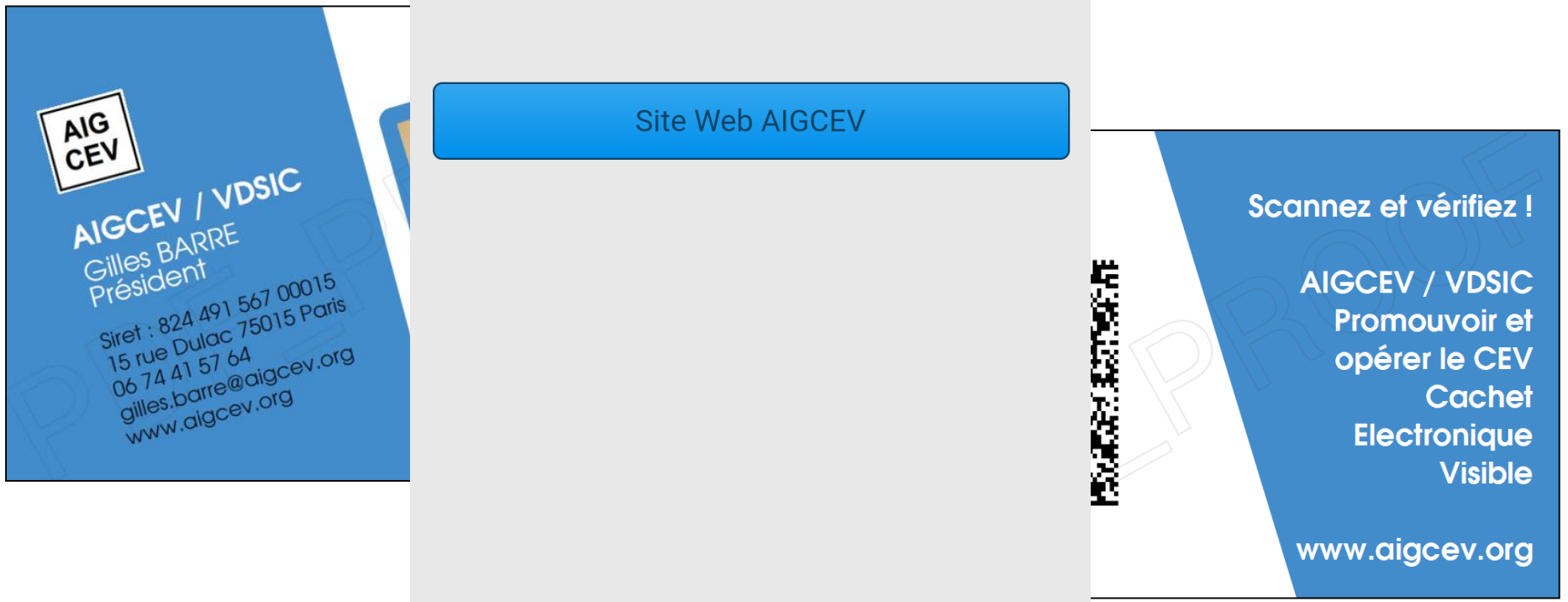
b) We have created the beginning of an international network, the *Otentik trusted network*.

Mrs Syrine TLILI, to whom I owe the honour of addressing you today, seized this object and implemented it in Tunisia in 2017 (securing salary slips for civil servants and diplomas).

In addition to Tunisia, VDS has been used in France since 2012, in more than 10 cases of public and private use

and by more than 20 issuers.

Experimental profile for the professional card.



Active demonstrator.

The volume of documents issued with the VDS will become very large as soon as the project to use them on accounting invoices is completed.

The interoperable OTENTIK VDS will be introduced in the next month in Canada, for documents from Notaries in the province of Québec.

Chambre des notaires

CERTIFICAT DE RECHERCHE DE DISPOSITIONS TESTAMENTAIRES

Certificat 123456789
émis le 2018-02-01 (A-M-J)

SPECIMEN POUR TEST
Les renseignements ici affichés ne sont pas représentatifs d'une situation réelle.
La version finale à venir de ce document pourrait être différente.

*Cachet électronique visible (CEV)

Recherche effectuée pour

Nom	Prénom	
Beaudoin	Éric	
1950-02-25 Date (A-M-J) ou année de naissance	123-456-789 Numéro d'assurance sociale	2018-01-17 Date du décès (A-M-J)

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla.

Résultat(s) de la recherche

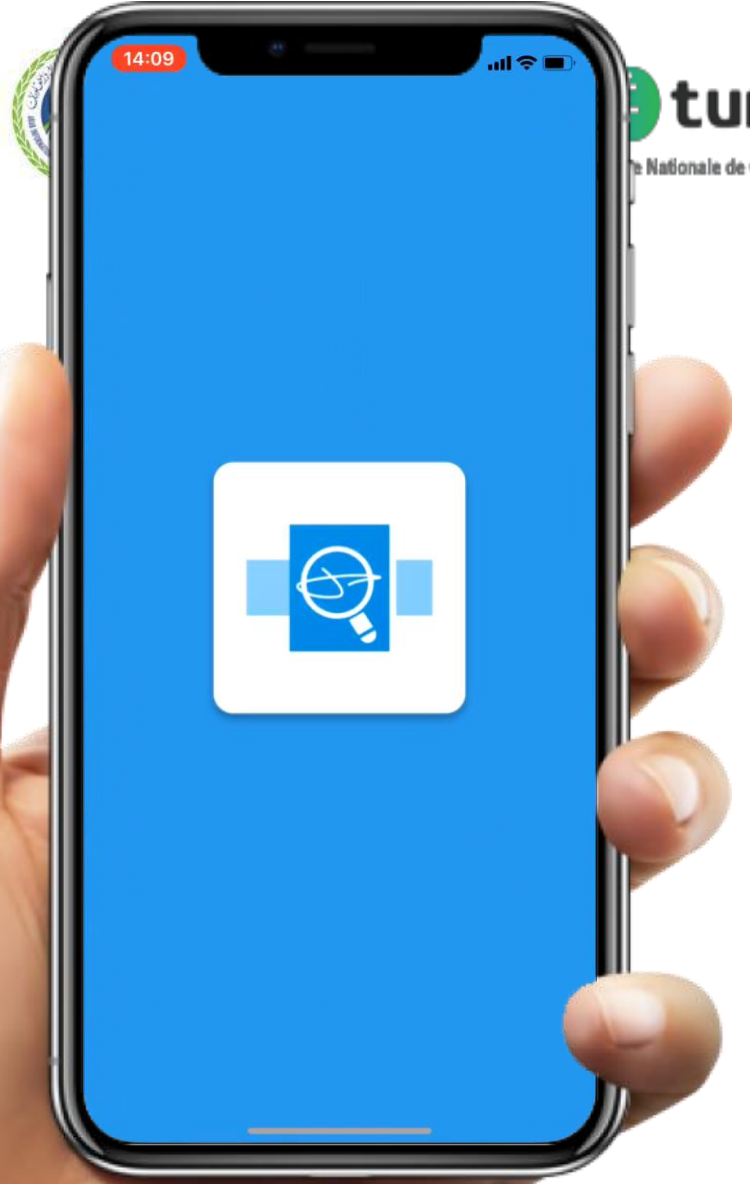
Inscription	Acte	Date (A-M-J)	Notaire instrumentant	Pour obtenir une copie de l'acte, communiquer avec
1 de 2	Codicille 123456	2012-06-25	Benoit Rivest	Richelieu Greffe C.S. 46 rue Charlotte Sorel QC J3P 6N5 450-742-2786
2 de 2	Testament 548759	1976-05-10	Benoit Rivest	Richelieu Greffe C.S. 46 rue Charlotte Sorel QC J3P 6N5 450-742-2786

Registraire
Chambre des notaires du Québec

* La vérification du cachet électronique visible (CEV), ou la vérification de la signature numérique apposée sur la version électronique du présent certificat de recherche, dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi.

101-2045, rue Stanley, Montréal QC H3A 2V4 Tel.: 514-879-1793 Toll free: 1-800-263-1793 cnc@cnq.org www.cnq.org

- Universal reader (mobile or web)
- Multilingual presentation view
  - With built-in functional code
- Signer’s legitimacy
- Data authenticity



Looking closely…

Classic HTML browsing.

Users are familiar with this. HTML is an open standard.

Logo and fonts are embedded in the html page to ensure a uniform view even offline.

Functional code in the presentation view.

The reader isn't aware of the business rule that requires a « Test » watermark for VDS signed with a test signature.

Multilingual

Did you notice the original document was in French? ☺

The *Otentik* network and VDS are unique

- **Universal reader, mobile or web**
- **Multilingual and uniform presentation views across devices**
  - **May include functional code and business rules**
  - **The presentation views and their descriptor are digitally signed & tamper proof**
- **Signer's legitimacy**
- **Data authenticity**
- **Long-term readability (decades)**
- **Open standards**

First use case on the *Otentik* network will be live in 6 weeks

The Open Standard was a hard requirement by the "*Chambre des Notaires du Québec*"

The top 3 differentiators have been tested :

1) **Signer's legitimacy**
2) **Uniform and multilingual presentation view with functional code, secured by a tamperproof digital signature**
3) **Universal reader, web or mobile**

The Approach (1)

Based on compatibility with existing projects (ANTS, BSI, ICAO, etc.)

The search for the best data compactness

The opening towards international standards

Standard XP Z42-101 is a Data Structure and not a system normative document.

The format with exclusion of governance was chosen with recommendations and an audit guide to imagine the appropriate governance.

The Approach (2)

This Standard is not a self-supporting part of a global system, it must be accompanied by governance, for example with regard to technical definitions of elements such as TSL, or compliance with certain regulations (like eIDAS for Europe).

To make the system working, it must follow a governance model based on this Format Standard. This is why VDSIC/AIGCEV was created to ensure the governance of private sector uses in France, and to promote uses whether they are national (Tunisia: ANCE) or governmental (ICAO).

Perspectives

- Propose an International Model for cross-sectoral use
- Technical Governance
- Trusted Environment Compliance :
  - Trusted Lists Federation
  - Trusted Entry Point (Universal Reader)
- Descriptor containing :
  - header information
  - type of encoding
  - reading structure
- Modes of cooperation with OTENTIK Network

If you are interested - join us !