Cybersecurity and .POST

27 May 2020

UNIVERSAL POSTAL UNION

Cosimo Birtolo
Chair of .POST Group
Poste Italiane

Víctor Martín González de Haro
Deputy Digital Business
Sociedad Estatal Correos y Telégrafos

Paul Donohoe
UPU Programme manager
Digital Economy and Trade

.POST

UNIVERSAL POSTAL UNION

The webinar is in ENGLISH – you may also chat in FRENCH

Participant phone lines will be MUTED (to reduce noise and interruptions)

Use the “CHAT” feature to ask QUESTIONS during the presentation

Questions will be answered after the speakers presentations

You will get the SLIDES and RECORDING by email after the session

POST

UNIVERSAL POSTAL UNION

TRUST & CYBERSECURITY

POST

A trusted space
managed by the UPU

Key points to cover

1. **Build trust** with .POST **secure** domain names
2. **Correos Spain** use of .POST for secure services

UNIVERSAL POSTAL UNION

POST

gives an new layer of cyber protection for your internet services

POST

UNIVERSAL POSTAL UNION

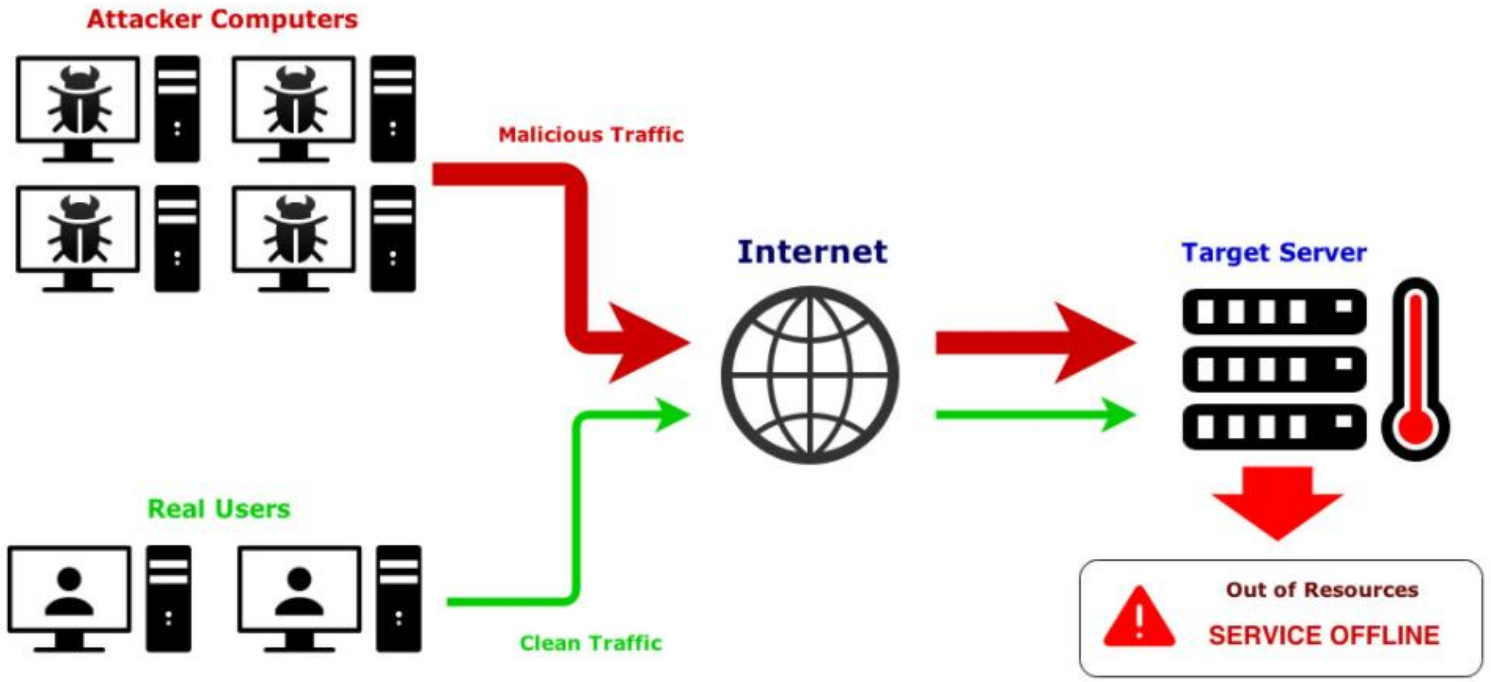
.POST PROTECTS YOU IN 5 WAYS

1) Protection against Denial of Service attacks (DDOS protection)
2) Protection against your domain being hijacked and spoofed (DNSSEC)
3) Protection against malicious emails from your domains (SPF and DKIM)
4) Encryption required for all .POST websites (HTTPS & TLS)
5) Verified domain (VERIFIED BY UPU)

Security monitoring of your domain name

POST

1) Protection against Denial of Service attacks



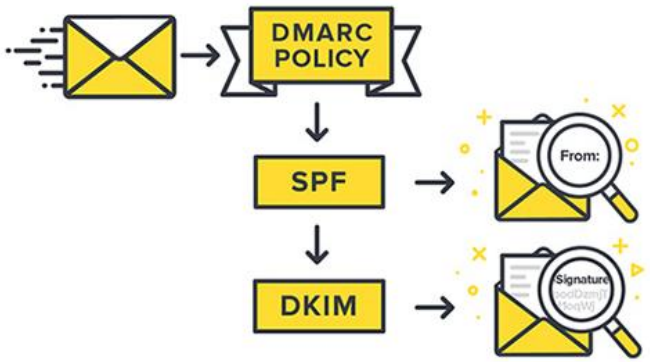
VALUE Minimize risks against DOS and DDOS

2) DNSSEC mandatory for all domains and subdomains under .POST

Policy	Benefits
All .POST domains must be signed using DNSSEC technology https://www.ietf.org/rfc/rfc4033.txt	**A chain of trust for the TLD and the domain**

VALUE **Minimize risks against website hijacking**

3) Protection against malicious emails from your domains – Security policies enforce SPF and DKIM



Policy	Benefits
All .POST domains with MX record should comply with the e-mail policy and use DKIM and SPF records https://tools.ietf.org/html/rfc6376 https://tools.ietf.org/html/rfc5585	**Improve the trust on e-mail under .POST**
Improved e-mail policy (DMARC mandatory implementation**)**	**Protecting your domain and reputation of your e-mail**

VALUE Increase the security and value of your brand and e-mail reputation

4) Encryption required for all .POST websites – Https & TLS 1.2

Policy	Benefits
Usage of TLS certificate version 1.2 or above + Headers	**Minimize cyberattacks (Man-in-the-middle)**
No domain redirection policy (except for CNAME records)	**MIM and SEO failover**

VALUE Ensure information transmitted from website is safe and secure

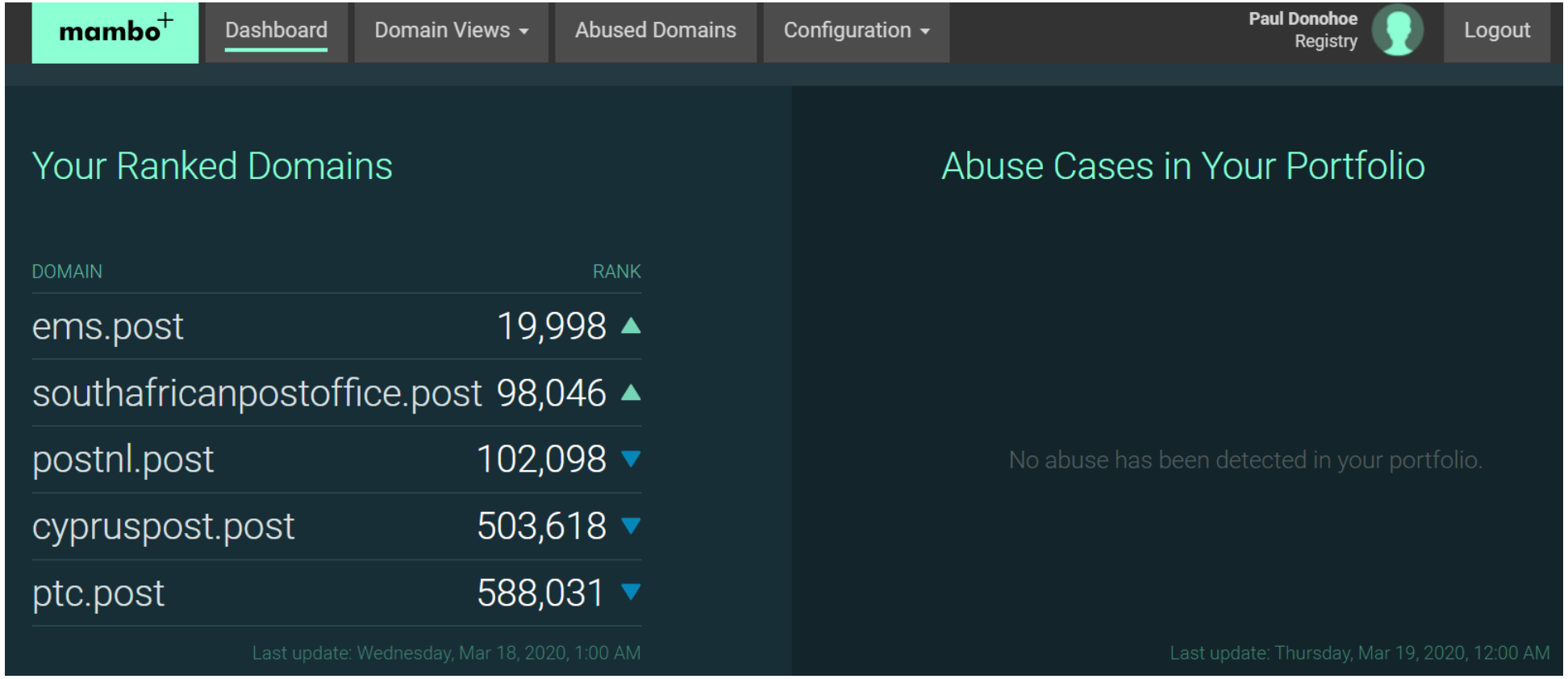
5) Verified domain

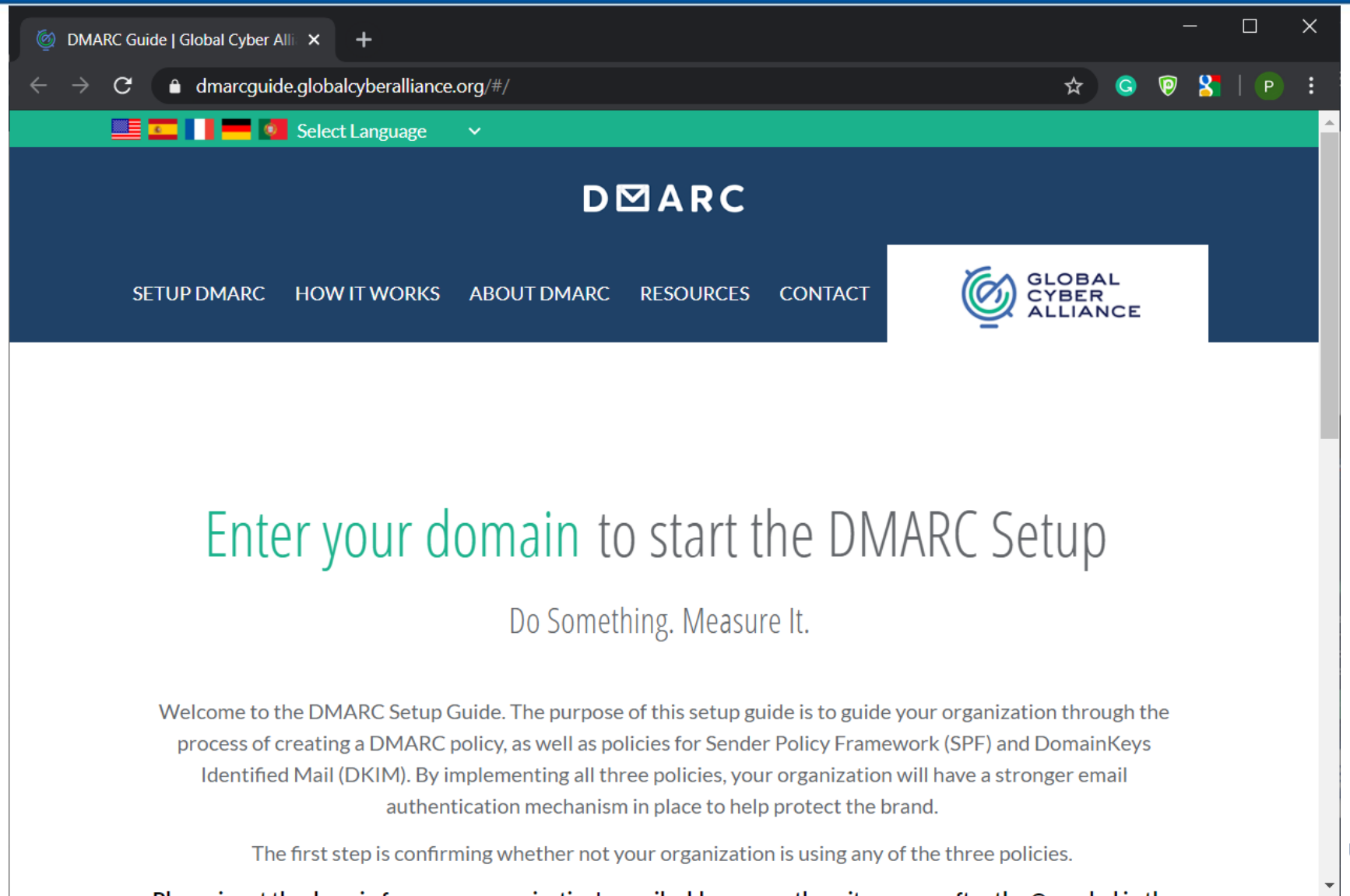
As a verified domain, bad actors simply cannot get a domain or email address that looks like yours to impersonate you and phish your employees and customers

VALUE **increase your website and brand protection**

Anti-abuse domain monitoring

It is important to monitor 24 X 7 abuse such as phishing, spam, botnets, and malware by continuously scanning different sources (third party and internal).





COMPLIANCE RESOURCES and TOOLS

These free resources can help understand whether the implementation of .POST domain names address our Security Requirements or identify potential issues that need to be resolved.

General (IPv6, DNSSEC, HTTPS, DMARC, DKIM, SPF, DANE)
https://internet.nl/site

Domain Name System Security Extensions (DNSSEC)

To confirm DNSSEC is deployed and configured properly at each zone and sub-zones for your .POST Domain, you can use these tools:
http://dnssec-debugger.verisignlabs.com/
http://dnsviz.net/

Email Authentication

To confirm the publication of DMARC or Sender Policy Framework (SPF) records in the DNS for your .POST Domain and the requested mail receiver policy of your DMARC record, you can use this tool:
https://www.internetsociety.org/ota/spf-dmarc-tools-record-validator
https://internet.nl/mail
https://dmarcian.com/dmarc-inspector

COMPLIANCE RESOURCES AND TOOLS (cont.)

To test your email server (i.e., MX record domain), the following tool will provide information about the configuration of your email server and whether it is using strong encryption practices:
https://www.paubox.com/secure-email-check

Transport Layer Security (TLS)/Encryption
TLS must be implemented to protect the integrity and confidentiality of data in transit.
The following tools allow you test the configuration of servers for TLS implementation:
https://www.checktls.com
https://www.htbridge.com/ssl
https://www.ssllabs.com/ssltest/analyze.html

Registrants must have a public key certificate (also known as digital identify or TLS certificates) in place to meet the HTTPS-only requirement. Registrants may wish to use a wildcard certificate (e.g., *.domainname.post) which covers every DNS name with encryption.
The following tool allows you to determine if the public key certificate installation has been successful:
https://www.digicert.com/help/

VALUE Minimize risks of DOS and DDOS attacks

VALUE Minimize risks against hijacking

VALUE Increase the security and value of your brand and e-mail reputation

VALUE Ensure information transmitted from website is safe and secure

VALUE Increase protection of your brand on the internet

UNIVERSAL POSTAL UNION

Correos case study

CORREOS at .POST

Víctor Martín González de Haro
Deputy Digital Business
Sociedad Estatal Correos y Telégrafos

POST

UNIVERSAL POSTAL UNION

List of Contents

.POST

UNIVERSAL POSTAL UNION

Why do we use .POST in Correos Spain

UNIVERSAL POSTAL UNION

.POST in Correos Spain

.POST A trusted space managed by the UPU

Security Users Trust

- ✓ .POST identify **LEGITIMATE** postal services and avoid confusion for Internet-users
- ✓ .POST is a **COMMUNITY-REGULATED TOP-LEVEL DOMAIN** (TLD), backed by the UPU's regulations, standards and legal framework.
- ✓ .POST is **SECURE**. All .POST web sites are DNSSEC secured. Internet users can trust that a .POST domain will not take them to an inauthentic web site.

.POST

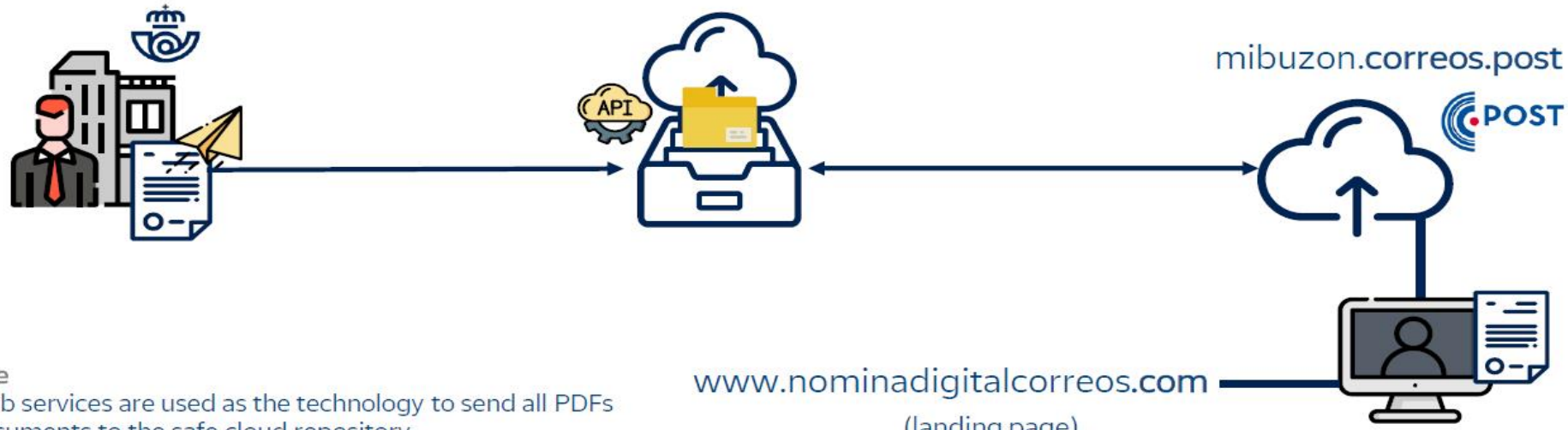
UNIVERSAL POSTAL UNION

What we have done with .POST in Correos Spain

Some use's cases with .POST domain

Correos Payrolls

CORREOS sends employee's payroll to a SAFE CLOUD REPOSITORY where each employee can access only to his/her documents



Secure

- Web services are used as the technology to send all PDFs documents to the safe cloud repository.
- Documents with password.
- Use DNSSEC

How to increase the security perception?
Employees access to their payrolls through .POST

.POST

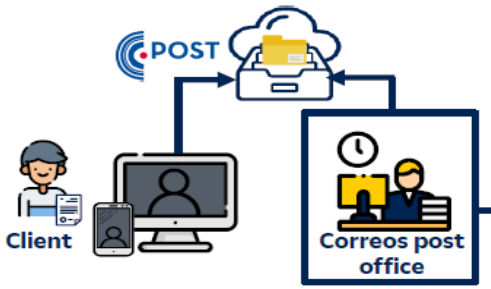
UNIVERSAL POSTAL UNION

Some use's cases with .POST domain

Business and Public Administrations' digital mailbox

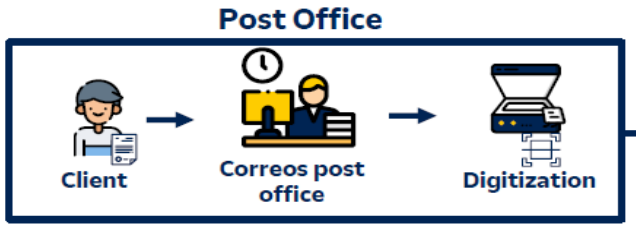
SENDERS SEND PAPER OR DIGITAL DOCUMENTS TO BUSINESS OR PUBLIC ADMINISTRATIONS FOR ANY TYPE OF REQUESTS

1 DIGITAL TO DIGITAL

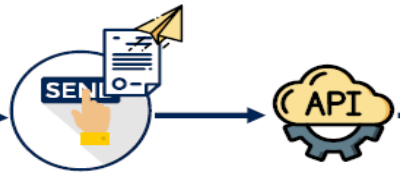


Client register and upload digital documents in cloud under a top level domain .POST and does to Correos post office to finalize sending process to recipients.

2 PAPER TO DIGITAL



Paper documents are digitized at Correos' post offices using a scanner and afterwards sent to the recipient's digital mailbox through a web service.



mibuzon.correos.post

.POST

Recipient's Mailbox

Universities, Government, etc. access to the digital mailbox located in cloud under a top level domain .POST

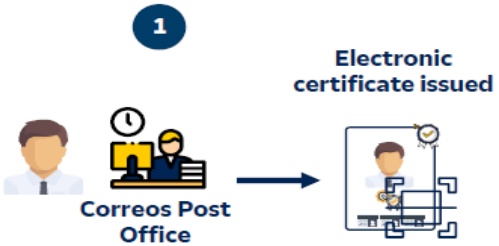
.POST

UNIVERSAL POSTAL UNION

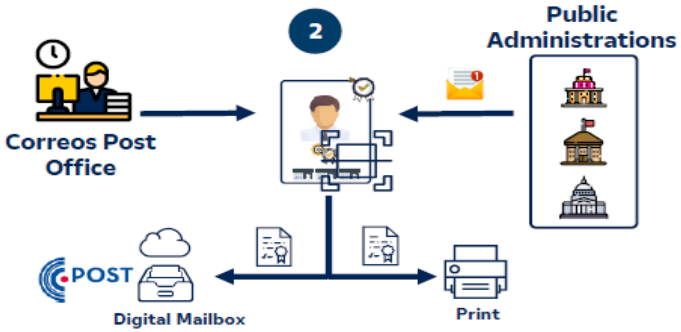
Some use's cases with .POST domain

Digital registered notifications*

CITIZENS AND NOT DIGITAL QUALIFIED PROFESSIONALS VISIT CORREOS POSTAL OFFICES TO CHECK AND STORE ALL PUBLIC NOTIFICATIONS ISSUED TO THEM BY PUBLIC ADMINISTRATIONS



- Correos as RA (Register Authority) verifies client's identity with ID card.
- Correos issues electronic certificate to the ID card verified.
- Certificates are stored is a safe cloud to be used at any time at Correos post offices.



- Correos application check all the sites where Public Administrations send their notifications using the client electronic certificate and put them together into a single client view.
- Notifications downloaded can be either printed at the office or sent to the client's digital mailbox under a .POST domain.

- Clients can afterwards access a safe web site under a top level domain .POST to check all transactions done at the post offices.

POST

*Available shortly

UNIVERSAL POSTAL UNION

Correos case study

CORREOS at .POST

Víctor Martín González de Haro
Deputy Digital Business
Sociedad Estatal Correos y Telégrafos

POST

UNIVERSAL POSTAL UNION

International Cooperation

GLOBAL CYBER ALLIANCE

ITU

CYBER READINESS INSTITUTE

Expert Knowledge

The Cyber Readiness Institute was founded by the CEOs of Mastercard, Microsoft, the Center for Global Enterprise, and PSP Partners, following their work on the Commission on Enhancing National Cybersecurity, to provide free tools and resources that your business can use to reduce risks. We believe that if we work together we can create a safer ecosystem for all businesses to thrive. Based on the expert input, the Program focuses on four critical cyber issues: Authentication and Passwords, Software Updates, Phishing, and USBs and Removable Media. The Program also includes guidance for implementing a practical cyber incident response plan.

POST

UPU UNIVERSAL POSTAL UNION

POST

DEFEND & DELIVER

DMARC

Email authentication for better email security

All IT and security practitioners are urged to join this technical bootcamp series with tools and resources to improve your email security.

ONLINE BOOTCAMP September 2020

GLOBAL CYBER ALLIANCE™

For more details:
Email: secretariat@info.post