Certified Electronic Mail (CEM)

draft-gennai-appsawg-cem-01.txt

francesco.gennai@isti.cnr.it
luca.frosini@isti.cnr.it
alba.shahin@isti.cnr.it
marina.buzzi@iit.cnr.it

What?
email system that allows a stronger proof of the exchange of communication between all participants.

Why?
Some user communities have perceived the need for more guarantees in email communication.

> Simply extra characteristics mainly for specific scenarios, not necessarily for common everyday use.

For what?
Official communications, contracts, etc.

Non repudiation and fair protocols for secure and reliable messaging.

We will refer to such a system as **Certified Electronic Mail** (**CEM**).

International Scenario

	Transport Protocol		Message Protocol	
	HTTP	SMTP	SOAP	eMail
PEC (Italy) [RFC6109]		X		X
DeMail (Germany)		X		X
DDS (Austria)	X		X	
Rpost Registered Email (USA)		X		X
Moja.posta.si (SI Post - Slovenia)	X		X	
PosteCS (Canada Post)	X		X	
ERV (Austria)	X		X	
REM (ETSI)		X		X
PReM (Universal Postal Union)	X		X	

None of them is compatible with the others. There are a lot of other examples: **PostX** (USA), **Goodmail**, **Tumbleweed**, **E-Postbrief** (Germany), **IncaMail** (Switzerland), **Apartado Postal Electronico** (Spain), **Certipost** (Belgium), **EuroNot@ries eWitness** (EU Notaries), **eNotarius eNmail** (Norway), **Certimail** (Spain), **EGVP** (Germany), **JUBES** (Netherland), **Notificaciones Electronicas** (Spain), **PRESTO** (France), **OCSI** (Germany) ...

Involved parties requirements

- Users
  - **Simple** : Use already known programs and avoid having to learn another method of operating.
  - **Interoperable** : Possibility to communicate with Internet standard email users.
  - **Uniform** : Use the same email address (mailbox) for certified and standard use.
- Providers
  - **Investment Saving** : Avoid implementing new solutions from scratch.
  - **Knowledge** : Operate with well-known technologies where they have a good know-how background, especially to face deployment and security issues.
  - **Value Added Service** : Enrich their offers to customers.

International Scenario

- **Required**
  - **Message Integrity**
  - **Evidences**
    - Non-Repudiation of Origin (**NRO**) (User ↔ Provider)
    - Non-Repudiation of Receipt (**NRR**) (User ↔ Provider)
    - Non-Repudiation of Submission (**NRS**) (User ↔ Provider)
    - User Non-Repudiation of Delivery (**U-NRD**) (User ↔ Provider)
    - **TimeOut** (User ↔ Provider)
    - Provider Non-Repudiation of Delivery (**P-NRD)** (Provider ↔ Provider)
- **Desiderata**
  - Confidentiality

Do we really need a CEM?

	Integrity	NRO	NRR	NRS	NRD	TimeOut
PEC (Italy) [RFC6109]	√^	w	-	√	√	√
DeMail (Germany)	√	w	-	√	√	√
DDS (Austria)	√	w	√	-	-	√
Rpost Registered Email (USA)	-	w	-	√	w	-
Moja.posta.si (SI Post - Slovenia)	√	√	√	-	-	√
PosteCS (Canada Post)	-	w	w	√	-	√
ERV (Austria)	√	w	x	-	√	√
REM (ETSI)	√	x*	x*	x*	x*	x*
PReM (Universal Postal Union)	√	√	√	√	√	x*
Internet eMail	°	°	-	-	-	-

Authenticity is guaranteed by NRO evidences if any.
Confidentiality is optional for all system.
w: Weak evidence. The system provides some kind of proof but they cannot be considered an NRx in the scientific sense of the term.
x* depend on the implementation.
° optional.
^ from sending provider to recipient.

Interoperability

- All the systems address the same issues in different way.
- Interoperability doesn't exist.

Thoughts

- Could an extension to DSN (Delivery Status Notification) [RFC3464] help us?
- Could an extension to MDN (Message Disposition notification) [RFC3798] help us?
- Could the definition of new email header fields be useful?
- Could the definition of new MIME types be useful?
- Could DKIM or SFP answer some of these issues?
- Are SMTP extensions necessary?

References

- [RFC1847] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC\01847, October 1995.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP\014, RFC\02119, March 1997.
- [RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC\03461, January 2003.
- [RFC3464] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC\03464, January 2003.
- [RFC3798] Hansen, T., Ed., and G. Vaudreuil, Ed., "Message Disposition Notification", RFC\03798, May 2004.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC\04949, August 2007.
- [RFC5598] Crocker, D., "Internet Mail Architecture", RFC\05598, July 2009.
- [RFC5617] Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)", RFC\05617, August 2009.
- [RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC\05750, January 2010.
- [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC\05751, January 2010.
- [RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", RFC\06376, September 2011.
- [RFC6109] Petrucci, C., Gennai, F., Shahin, A., and A. Vinciarelli, "La Posta Elettronica Certificata - Italian Certified Electronic Mail", RFC\06109, April 2011.
- [TAUBER] Arne Tauber, "A survey of certified mail systems provided on the Internet," Computers & Security, vol. 30, no. 6-7, pp. 464-485, September-October 2011.
- [T-CHIMP] Thinking Chimp : http://blogdramedy.files.wordpress.com/2011/04/thinking-chimp.jpg?w=234&h=300