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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Message Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEC (Italy) [RFC6109]</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DeMail (Germany)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DDS (Austria)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Rpost Registered Email (USA)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Moja.posta.si (SI Post - Slovenia)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PosteCS (Canada Post)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ERV (Austria)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>REM (ETSI)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>PReM (Universal Postal Union)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

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?

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

**Authenticity** is guaranteed by NRO evidences if any.

**Confidentiality** is optional for all systems.

- **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

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP\014, RFC\02119, March 1997.