**Change Request**

**for the update of ISO 20022 financial repository items**

1. **Origin of the request:**

*A.1 Submitter*: nexo A.I.S.B.L

*A.2 Contact person:* Philippe CECE ([Philippe.cece@ingenico.com](mailto:Philippe.cece@ingenico.com)) / Laure BELTRI ([laure.beltri@frenchsys.com](mailto:laure.beltri@frenchsys.com))

*A.3 Sponsors*: nexo A.I.S.B.L.

1. **Related messages:**

* CertificateManagementRequest V05
* CertificateManagementResponse V05
* MaintenanceDelegationRequest V08
* MaintenanceDelegationResponse V06

1. **Description of the change request:**

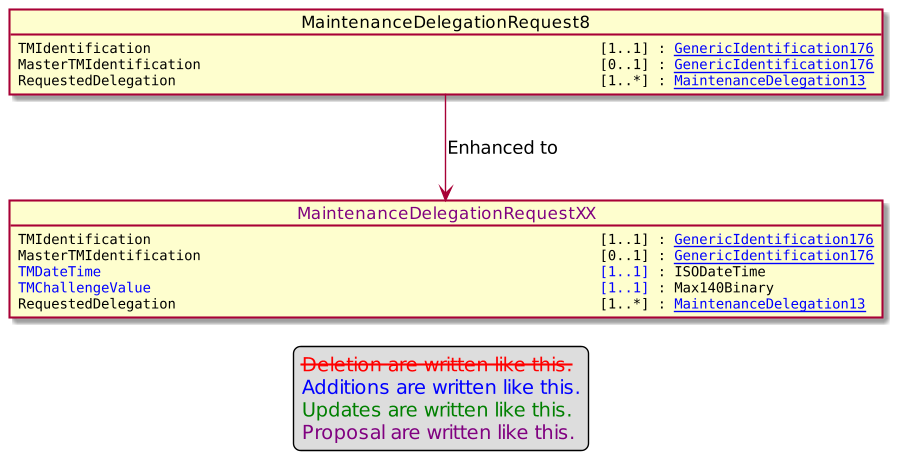
After a study, we realize that, in some circumstances like using some cryptographic algorithms without respect to best practices, some TMS message bodies are not protected against a replay attack.

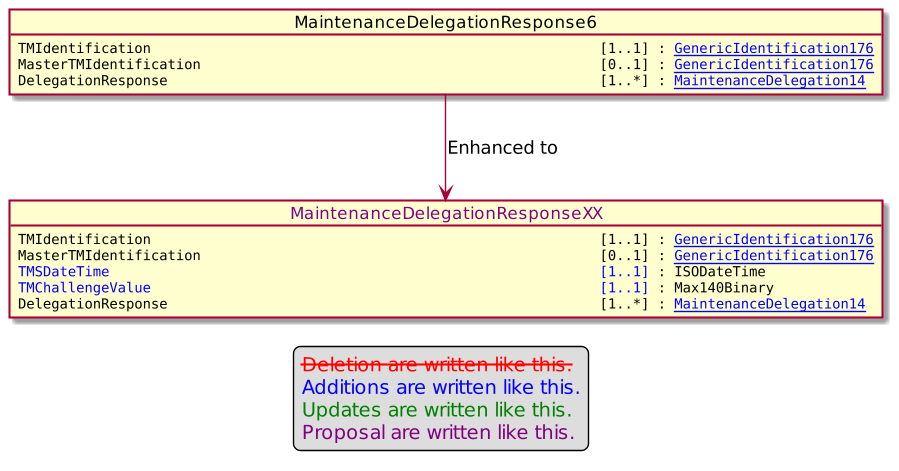
The aim of this Change request is to avoid this by adding elements like date and challenge that will avoid considering messages sent by a replay attack.

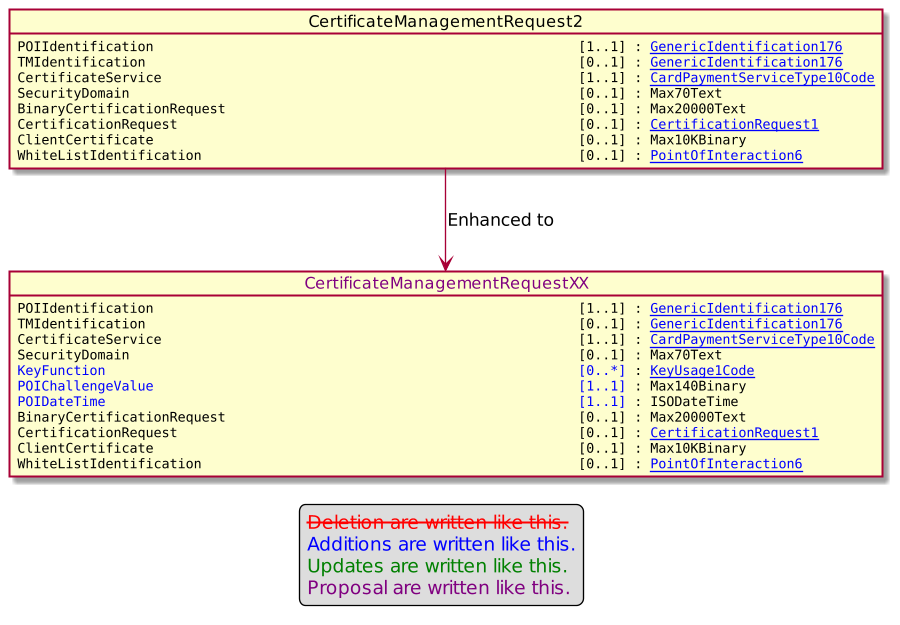
We take also this opportunity to clearly identify in the *CertificateManagementRequest* message, the *KeyFunction* since this information should be present in a certificate returned by the *CertificateManagementResponse*.

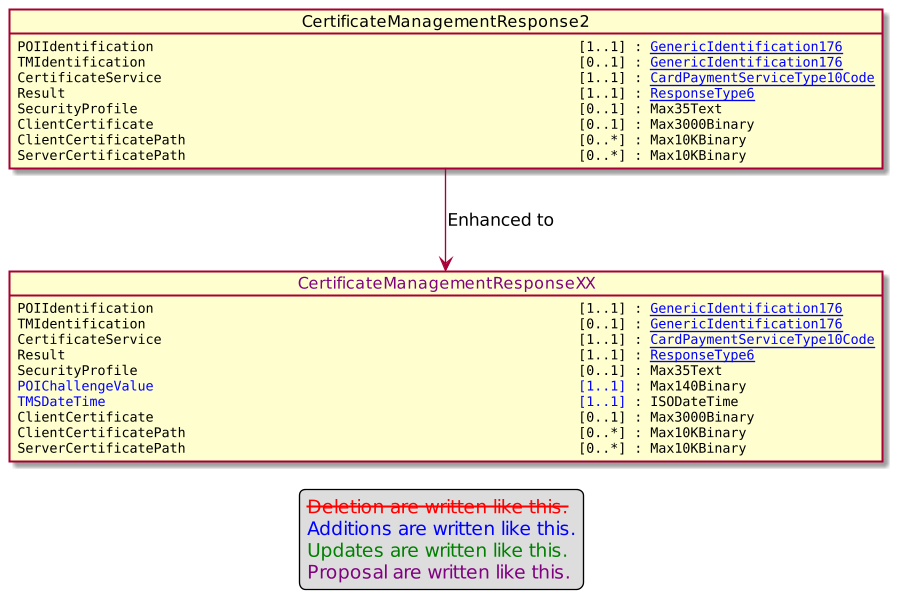
1. **Purpose of the change:**

The following diagrams identify the message components that will be updated and the added message elements coupled with their type.









1. **Urgency of the request:**

Urgent.

1. **Business examples:**
2. **SEG/TSG recommendation:**

*This section is not to be taken care of by the submitter of the change request. It will be completed in due time by the SEG(s) in charge of the related ISO 20022 messages or the TSG for changes related to the BAH.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Consider** | |  | **Timing** |  |  |  |
|  |  | | - **Next yearly cycle: 2022/2023**  (the change will be considered for implementation in the yearly maintenance cycle which starts in 2022 and completes with the publication of new message versions in the spring of 2023) | |  |  |
|  |  | | - **At the occasion of the next maintenance of the messages**  (the change will be considered for implementation, but does not justify maintenance of the messages in its own right – will be pending until more critical change requests are received for the messages) | |  |  |
|  |  | | - **Urgent unscheduled**  (the change justifies an urgent implementation outside of the normal yearly cycle) | |  |  |
|  |  | | - **Other timing:** | | |  |

Comments:

|  |  |
| --- | --- |
| **Reject** |  |

Reason for rejection: