Enable secure hardware tokens

Proposal for WebCrypto.Next

Gemalto

Requirements

- Enable users to use their secure hardware tokens with web applications
  - E.g. authenticate to a website, sign a transaction, encrypt a file
- Use hardware tokens to do crypto operations and random number generations
- Use hardware tokens to generate keys and certificates, and store them inside the tokens
- Allow discovery of tokens and keys/certificates stored in the tokens

Proposal

- A secure hardware token registers as a CryptoProvider
- Get CryptoProviders from Window (or another object)
- A CryptoProvider has
  - Crypto
  - getKeys (get key handles)
  - Certificate management
- Crypto has methods as defined in WebCryptoAPI:
  - getRandomValues
  - SubtleCrypto
  - All operations run in the context of the CryptoProvider
- Default CryptoProvider is browser's native support as currently with WebCryptoAPI

Proposal – top level API

```
partial interface Window {
        Promise<any>    getCryptoProviders();
}
Interface CryptoProvider {
        DOMString    Id;
        readonly  attribute  CryptoProviderType   type; //Default, SE, TEE, TPM, etc.
        readonly  attribute  Crypto                 crypto; // defined in WebCryptoAPI
        Promise<any>    getKeys  (
                            AlgorithmIdentifier   algorithm,
                            KeyUsage              usage
        );
        Promise<any>    getCertificates  (
                            DOMString             issuer,
                            DOMString             subject,
                            CertificateUsage      usage
        );
        … … // other certificate management methods, e.g. import, remove, etc.
}
```

References

This proposal

- Uses W3C WebCrypto API
- Was inspired by Chrome.enterprise.platformKeys API
- Is complementary with Microsoft certificate and key management requirements and proposal
- May extend WebCrypto Key Discovery