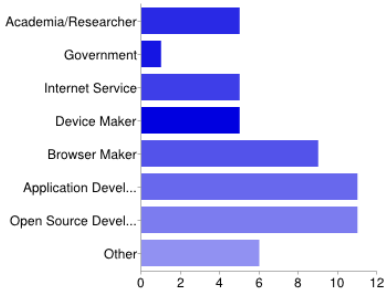
37 responses

Summary See complete responses

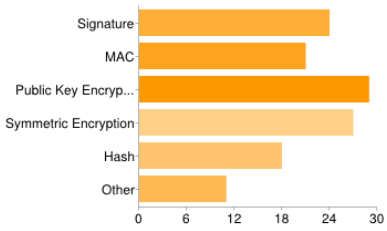
What industry or organization are you involved with?



Academia/Researcher	5	18%
Government	1	4%
Internet Service	5	18%
Device Maker	5	18%
Browser Maker	9	32%
Application Developer	11	39%
Open Source Developer	11	39%
Other	6	21%

People may select more than one checkbox, so percentages may add up to more than 100%.

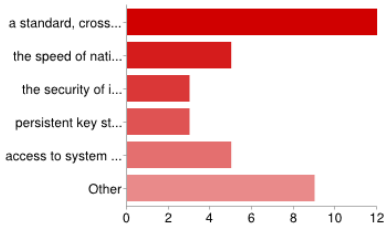
What methods of the Crypto API are you most interested in?



Signature	24	65%
MAC	21	57%
Public Key Encryption	29	78%
Symmetric Encryption	27	73%
Hash	18	49%
Other	11	30%

People may select more than one checkbox, so percentages may add up to more than 100%.

Why are you interested in a Web Crypto API?



a standard, cross-browser API	12
the speed of native crypto implementation	5
the security of isolating the keys from JavaScript code	3
persistent key storage	3
access to system cert/key store (e.g., Mac OS X Keychain) or smart cards, or other system or browser resources not accessible to JavaScript today	5
Other	9

Are you interested in a high-level, idiot-proof API or a low-level API?

Low-level High-level, idiot-proof High-level, idiot-proof Low-level Low-level Low-level Low-level High-level, idiot-proof Both. Power users obviously need low-level APIs to consume custom (read: already existing) services. However, there is a lot that could go wrong in implementations if only low-level APIs are provided. A high-level API for common tasks (like symmetric encryption) I consider to be a must-have. People are going to implement this anyway. So, you might as well provide a "batteries included" solution that covers the 95% and that people can rally behind as a standard way of doi ...

In your planned usage, who are the users of this API?

Application like webex are interested in making sure that data can be encrypted from one end users browser to the other ends users browser without the web servers in the middle (like webex) having access to the data. Non-Crypto Web App Developers Financial transactions such as banking, cyber trading and credit card processing Developers (experienced) Primarily web application developers Cable Television Interactive Application Developers Netflix security software engineers porting / creating our own RESTful protocol security to generic web browsers and beyond. Digital certificate Authorities pr ...

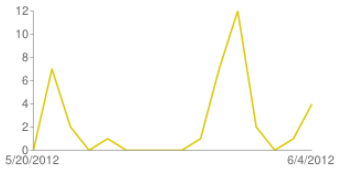
What data is being processed/encrypted/signed, etc?

Small text messages such as IM style chat. Larger chunks of data that represent documents such as as slides. User Entered Data intended to be hidden from the server data in web applications for financial transactions Signed, encrypted - Commercial documents Encrypted - Local data from HTML5 applications and other files Authentication data (to verify user or device) Digital media content that needs to be decrypted Application data that needs to be signed Audio/Video/Application data Arbitrary device <-> server protocols. At present the data includes: device authentication data, user authenticati ...

Why is this data being processed/encrypted/signed, etc?

The webex application is trying to help two users Alice and Bob, collaborate, but Alice and Bob do not want to share the information with webex. The goal is not to stop webex from attacking Alice and Bob but to allow Alice and Bob to verify a promise that webex did not do this. It is more about detection than stopping it from happening. You can imagine a solution where webex helps distribute public keys, and users can check those out of bound if desired. In an Honest but Coercible or Honest but Curious threat model, the server will store users data, but should not be able to read it. Thi ...

Number of daily responses


12
10
8
6
4
2
0
5/20/2012
6/4/2012