From: Iorga, Michaela
To: Chen, Lily
Cc: Perlner, Ray; Moody, Dustin
Subject: Re: Keyless signature infrastructure
Date: Friday, January 8, 2016 4:36:23 PM
Attachments: Fwd Four decks for NIST.msg

Hi Lily,
Thank you for your reply. I am attaching the email with the presentations given to Crypto team a year ago – in case the material is of more interest now than in 2014. Meltem might have copies too.

I keep seeing them in the news spreading their technology around the world and in US, with the defense community. Since DoD is moving more and more to NIST standards, I thought we could be proactive on their behalf :). I am glad to hear NIST is.

Michaela

From: "Chen, Lily" <lily.chen@nist.gov>
Date: Friday, January 8, 2016 at 9:23 AM
To: "Iorga, Michaela" <michaela.iorga@nist.gov>
Subject: Re: Keyless signature infrastructure

> Michaela:
>
> Happy New Year!
>
> Thank you for the information. If I understand right, the so-called keyless signature infrastructure is one of the hash based signatures. It is NOT keyless. It is essentially a one-time signature. That is, a private key can use only once. Currently, this kind of signatures has been considered in the category of "post quantum cryptography". We have a team working on it led by Dustin Moody and Yi-Kai Liu.
>
> There are certain issues due to its one time signature feature, which is called stateful signature. There are some stateless versions. But the signature size is still far too large compared with the signature schemes we have deployed, like RSA.
>
> There are some IETF drafts on hash based signatures. Your officemate, Ray, is knowledgeable on this. You may like to chat with him.
>
> In summary, the community is still working on it. NIST has been closely involved.
>
> Lily

From: Iorga, Michaela
Sent: Tuesday, January 5, 2016 11:30 AM
To: Chen, Lily
Subject: Keyless signature infrastructure

Lily,
Happy New Year to you!

I saw an article today that made me think that I should share it with you and ask if you think NIST should look into Keyless Signature Infrastructure (KSI) - a block chain technology that provides massive-scale data authentication without reliance on centralized trust authorities. If defense agency are interested, maybe federal gov agency at large could use it too if NIST approves it. Please see some information below. The company was at NIST and presented their work more than a year ago.
http://www.ibtimes.co.uk/security-firm-guardtime-courting-governments-banks-keyless-blockchain-1535835

Security firm Guardtime courting governments and banks ...

www.ibtimes.co.uk

Guardtime is a cyber-security provider that uses blockchain systems to ensure the integrity of data. It most recently applied its technology to protect the UK's ...

Michaela