Xen Shell - Feature # 211: Support FIDO2 SSH ecdsa-sk/ed25519-sk keys for console access

Status:	Resolved	**Priority:**	Normal
Author:	halleck	**Category:**	
Created:	2023-05-28	**Assigned to:**	
Updated:	2023-06-02	**Due date:**	
Subject:	Support FIDO2 SSH ecdsa-sk/ed25519-sk keys for console access		
Description:	It would be nice if Bitfolk's VPS console access supported FIDO2 SSH ecdsa-sk/ed25519-sk keys. Personally I'm currently in the process of migrating from doing GPG-SSH to FIDO2-SSH, and it would appear as if the BitFolk VPS console will be my only holdover. Assuming that you trust the console hosts to use the buster-backports repository, it currently provides OpenSSH 8.4, which ought to have the needed support.		

History

2023-05-28 12:19 - admin

On the sshd side, does @PubKeyAuthOptions@ need to be set and contain @touch-required@ or @verify-required@? Or will that be set in the line you add to @authorized_keys@ file (via the Psnel)?

https://manpages.debian.org/bullseye/openssh-server/sshd_config.5.en.html#PubkeyAuthOptions

2023-05-28 13:02 - halleck

Here's how I have understood it...

The default behavior is that touch/presence is required, unless @no-touch-required@ is specified in authorized_keys. Except that by specifying @touch-required@ in sshd_config you override any potential authorized_keys @no-touch-required@.

For pin/verify the default is that it isn't required, but that it can be made a must either system wide by setting @verify-required@ in sshd_config or key wise by setting @verify-required@ in authorized_keys.

2023-05-28 13:19 - admin

So I think that means to not set it on server side, but do optionally allow @verify-required@ in the @authorized_keys@ line?

2023-05-28 13:51 - halleck

Yepp, that seems like the sane approach for Bitfolk's VPS console access.

2023-06-01 21:44 - admin

SSH has now been updated and the Panel now allows keys of types:
* sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,
* sk-ecdsa-sha2-nistp256@openssh.com
* sk-ssh-ed25519@openssh.com

to be added, so could you give this a go now?

2023-06-02 03:39 - halleck

Just added my sk-ssh-ed25519@openssh.com key,and it worked like a charm.

Managed to access the Xen shell both hobgoblin and on leffe.

Thanks!

2023-06-02 04:22 - admin

- Status changed from New to Resolved