CURDLE WG

IETF99

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- **The IETF plenary session**
- **The IESG, or any member thereof on behalf of the IESG**
- **Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices**
- **Any IETF working group or portion thereof**
- **Any Birds of a Feather (BOF) session**
- **The IAB or any member thereof on behalf of the IAB**
- **The RFC Editor or the Internet-Drafts function**

All IETF Contributions are subject to the rules of RFC 5378All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Table of Content

- WG document status
- draft-ietf-curdle-ssh-kex-sha2-08
- Where are we ?

WG documents status since IETF98

CMS: (default sent to IESG)

- draft-ietf-curdle-cms-ecdh-new-curves-09
- draft-ietf-curdle-cms-eddsa-signatures-06

Kerberos:

- draft-ietf-curdle-des-des-des-die-die-die-03
- draft-ietf-curdle-gss-keyex-sha2-02 (WGLC)

PKIX:

- draft-ietf-curdle-pkix-05
- draft-schaad-curdle-oid-registry-01 (WGLC)

WG documents status since IETF98

SSH: (default sent to IESG)

- draft-ietf-curdle-rsa-sha2-09
- draft-ietf-curdle-ssh-curves-05
- draft-ietf-curdle-ssh-dh-group-exchange-04
- draft-ietf-curdle-ssh-ext-info-10
- draft-ietf-curdle-ssh-kex-sha2-08 (WGLC)
- draft-ietf-curdle-ssh-modp-dh-sha2-07

Other:

- draft-ietf-curdle-rc4-die-die-die-00 (WG adoption)

draft-ietf-curdle-ssh-kex-sha2-08

Key Exchange Method Name	Reference	Implement
curve25519-sha256	ssh-curves	SHOULD+
diffie-hellman-group-exchange-sha1	RFC4419	MUST NOT
diffie-hellman-group1-sha1	RFC4253	MUST NOT
diffie-hellman-group14-sha1	RFC4253	SHOULD-
diffie-hellman-group14-sha256	new-modp	MUST
diffie-hellman-group16-sha512	new-modp	SHOULD+
ecdh-sha2-nistp256	RFC5656	SHOULD-
ecdh-sha2-nistp384	RFC5656	SHOULD+
gss-gex-sha1-*	RFC4462	MUST NOT
gss-group1-sha1-*	RFC4462	MUST NOT
gss-group14-sha1-*	RFC4462	SHOULD-
gss-group14-sha256-*	gss-keyex	SHOULD
gss-group16-sha512-*	gss-keyex	SHOULD+
rsa1024-sha1	RFC4432	MUST NOT

Where are we ? - Charter

"The set of cryptographic mechanisms that can be introduced are limited to key agreement (ECDH) and digital signatures (EdDSA) with Curve25519 and Curve448 as defined by CFRG [1] [2], and the AEAD mode ciphers consisting of ChaCha20 and Poly1305 also defined by CFRG [3]. Other variants of mechanisms, such as the ChaCha20-Poly1305 construct deployed for SSH, may also be considered as well as AES-CCM[4] and AES-GCM [5] where those are not already defined and where there is implementer interest. Related specifications such as private and public key formats are also within scope.

The protocols the WG intends to work on are SSH, DNSSEC, PKIX, CMS, XML Digital Signatures and potentially XML Encryption, Kerberos and JSON ."

[1] https://tools.ietf.org/html/draft-ietf-curdle-ssh-ed25519-00
[2] https://www.ietf.org/mail-archive/web/jose/current/msg05357.html

Where are we ? - Ed*/X*...

	Ed25519/Ed448	X25519/X448	Chacha20Poly1305	AES-GCM	AES-CCM
SSH	Draft-ietf-curdle-ssh-ed25519-00 (TBD)	draft-ietf-curdle-ssh-curves-05	TBD	RFC5647	TBD
DNSSEC	RFC8080 (curdle)	NA	NA	NA	NA
PKIX	draft-ietf-curdle-pkix-05 draft-schaad-curdle-oid-registry-01		NA	NA	NA
CMS	draft-ietf-curdle-cms-eddsa-signatures-06	draft-ietf-curdle-cms-ecdh-new-curves-09	RFC 8103 (curdle)	RFC5084	RFC5084
XML					
Kerberos		draft-ietf-curdle-gss-keyex-sha2-02	TBD	TBD	TBD
JSON	Msg05357 (TBD)				

Where are we ? - Sig/DH/Updates

	New Signature	New DH	Deprecation / Crypto Recommendations
SSH	draft-ietf-curdle-rsa-sha2-09 draft-ietf-curdle-ssh-ext-info-10	draft-ietf-curdle-ssh-modp-dh-sha2-07	draft-ietf-curdle-ssh-dh-group-exchange-04 draft-ietf-curdle-ssh-kex-sha2-08
DNSSEC	NA	NA	draft-arends-dnsop-dnssec-algorithm-update-00 (DNSOP) Draft-wouters-sury-dnsop-algorithm-update-02 (DNSOP)
PKIX	NA	NA	
CMS	NA	NA	
XML			
Kerberos		draft-ietf-curdle-gss-keyex-sha2-02	draft-ietf-curdle-rc4-die-die-die-00
JSON			

Thanks!