GIS
ГАЗИНФОРМ СЕРВИС

Актуальные вопросы сравнения протоколов сервисов проверки электронной подписи

Ермина Екатерина
Ведущий инженер

Кирюшкин Сергей
Советник генерального директора –
начальник удостоверяющего центра

PKI Forum 2023
12-14 сентября 2023 года
Санкт-Петербург

GIS
ГАЗИНФОРМ
СЕРВИС

Содержание доклада

02

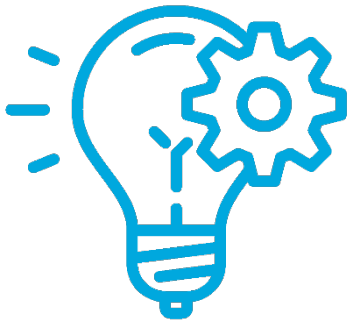
- Предпосылки к сравнению протоколов сервисов проверки ЭП
- Обзор протокола OASIS DSS
- Сравнение протоколов
- Международный опыт

GIS
ГАЗИНФОРМ
СЕРВИС

03

Предпосылки к сравнению протоколов сервисов проверки электронных подписей

- Актуализация сравнительного анализа протоколов проверки электронных подписей
- Практика применения сервиса проверки электронных подписей
- Обмен новыми форматами электронных документов



GIS
ГАЗИНФОРМ
СЕРВИС

Обзор протокола OASIS DSS

04

- устранены ошибки и известные уязвимости протокола
- учтены требования к протоколу, ставшие известными в процессе его применения
- упрощена базовая схема, путем исключения редко используемых элементов
- выполнена поддержка синтаксисов, отличных от XML
- включены профили для описания обработки нескольких подписей, благодаря изменению мощность объектов подписи на «неограниченную»

GIS
ГАЗИНФОРМ
СЕРВИС

Обзор протокола OASIS DSS

05

Протокол OASIS DSS предназначен для создания и проверки:

- XML-подписей [XMLDSIG]
- CMS-подписей [RFC 3852]
- XML-штампов времени
- штампов времени в соответствии с RFC 3161
  (в том числе в составе CAdES, XAdES, PAdES)

GIS
ГАЗИНФОРМ
СЕРВИС

Сравнение протоколов

06

Параметр	OASIS DSS	RFC 3029 DVCS
Виды запросов	• создание ЭП электронного документа; • проверка валидности ЭП; • запрос на предоставление информация о времени подписания электронного документа	• удостоверение обладания данными (cpd); • удостоверение обладания данных без их предоставления сервису (ccpd); • проверка валидности ЭП ЭД(vsd); • проверка валидности сертификата (vpkc)
Транспортный протокол	• HTTP POST • TLS • SOAP	• HTTP POST • TLS • S/MIME
Тип подписи, которую можно проверить	• XML-подпись [XMLDSIG] • CMS-подпись [RFC 3852] • XML-штамп времени • штамп времени в соответствии с RFC 3161	• CMS-подпись [RFC 3852] • Усовершенствованные ЭП (ETSI EN 319 132 (XAdES), ETSI EN 319 122 (CAdES), ETSI EN 319 142 (PAdES))

GIS
ГАЗИНФОРМ
СЕРВИС

Сравнение протоколов

Параметр	OASIS DSS	RFC 3029 DVCS
Формат ответа	XML-документ, подписанный электронной подписью	Ответ с CMS-подписью (CAdES)
Возможность проверки подписи без предоставления самого документа	Да	Да*
Возможность проверки двух и более подписей	Да	Да
Применимость протокола для проверки иностранной подписи	Да	Да
Релизация протокола у сторонних ДТС	Да (сервисы валидации ЕС в соответствии с eIDAS, VA)	Да (служба ДТС ЕАЭС, ДТС в РФ, Казахстане, Беларуси, Армении, пилотные ДТС Азербайджана и КНР)

GIS
ГАЗИНФОРМ
СЕРВИС

08

Международный опыт

ETSI TS 119 442 V1.1.1 (2019-02)

Electronic Signatures and Infrastructures
Protocol profiles for trust service providers
AdES digital signature validation serv

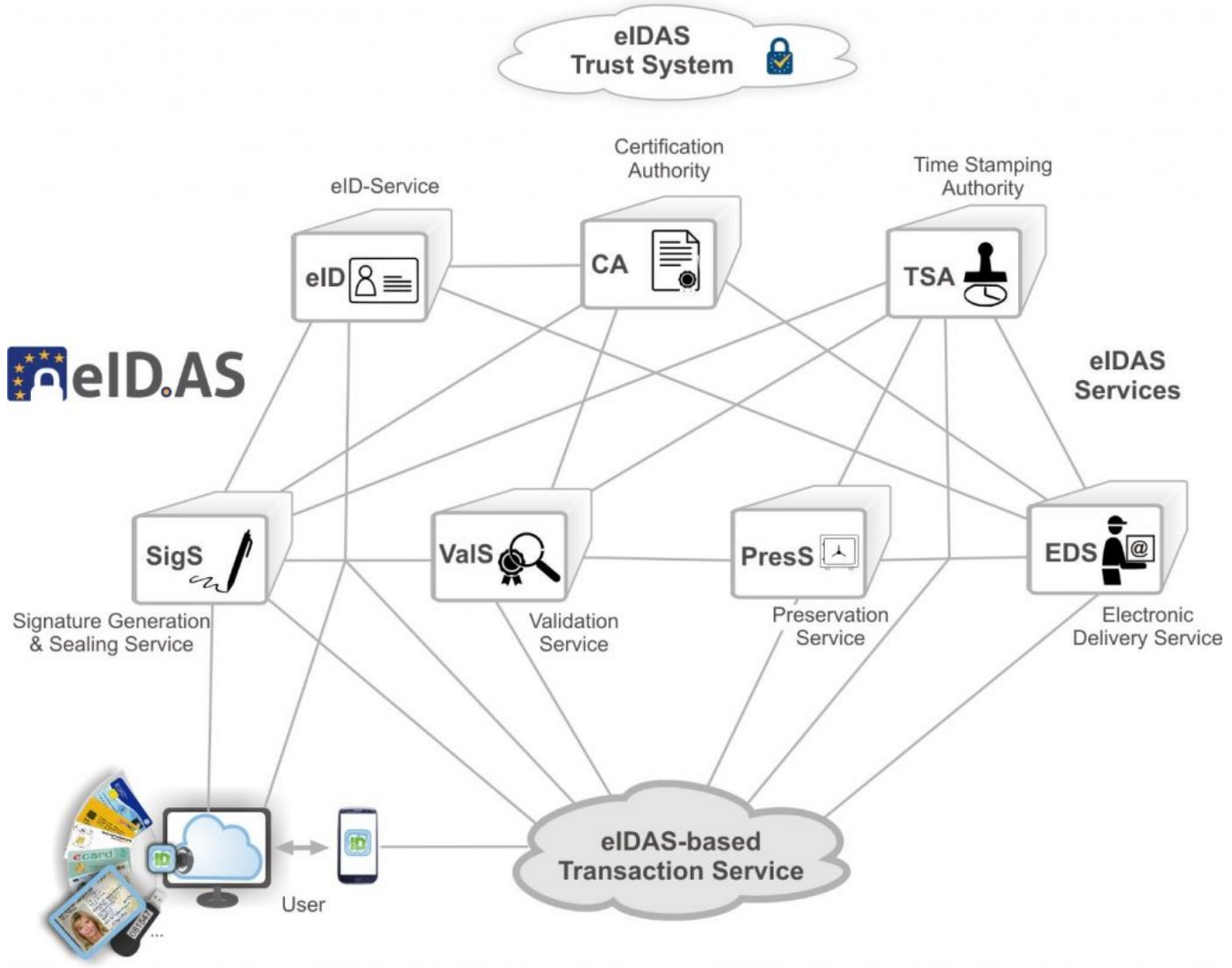
ETSI TS 119 432 V1.1.1 (2019-03)

Electronic Signatures and Infrastructures (ESI);
Protocols for remote digital signature creation

GIS
ГАЗИНФОРМ
СЕРВИС

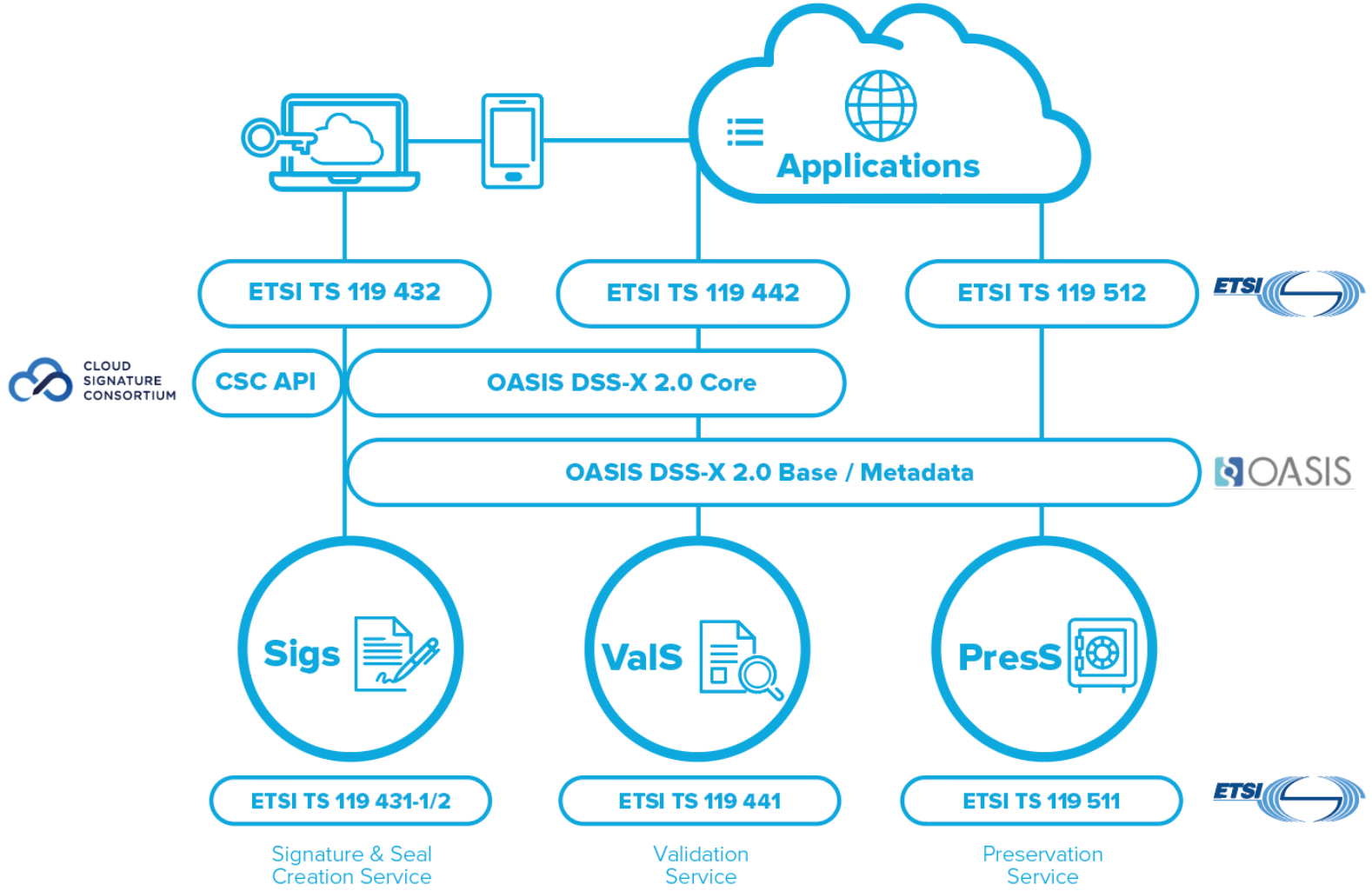
11

Международный опыт



GIS
ГАЗИНФОРМ
СЕРВИС

Международный опыт



GIS
ГАЗИНФОРМ
СЕРВИС

Заключение

GIS
ГАЗИНФОРМ
СЕРВИС

Спасибо
За внимание!

Ермина Екатерина
Ведущий инженер

ermina-e@gaz-is.ru

Кирюшкин Сергей
Советник генерального директора –
начальник удостоверяющего центра

kiryushkin-S@gaz-is.ru

www.gaz-is.ru