
# Возможные подходы по созданию единых правил и рекомендаций по построению общего пространства идентификации стран СНГ на основе рекомендаций ITU-T

Региональный семинар стран СНГ
“Развитие электронного правительства как одно из условий интеграции в глобальное информационное общество”
Москва 25-27 ноября 2013г.

Игнатьева М.А. –Эксперт Российской Федерации
ignatm90@mail.ru

ISO 3166-1 *Codes for the representation of names of countries and their subdivisions*

Recommendation ITU-T, *Abstract Syntax Notation One (ASN.1)*, X.680

С глубоким уважением к сообществу МКТТ, МСЭ, ITU-T, ISO

От 1974 года

К 2014 году

Recommendation ITU-T, *The directory* : X.500, X.509, X.520

Recommendation ITU-T, *Registration of object identifier..* X.660, X.662,X.666, X.668, X.669, X.672

**ISO 3166-1** ***Codes for the representation of names of countries and their subdivisions***

Коды для стран (В соответствии с бюллетенем ООН, начало формирования 1974г.):

| | | | | | |
|---|---|---|---|---|---|
| Белоруссия: | BY | 112 | Молдова: | MD | 498 |
| Россия : | RU | 643 | Казахстан: | KZ | 398 |
| Украина: | UA | 804 | Киргизстан: | KG | 417 |

**Recommendation ITU-T,** ***Abstract Syntax Notation One (ASN.1)*** **X.680 Взаимосвязь открытых систем.**

Спецификация абстрактно-синтаксической нотации версии один (АСН.1) ГОСТ Р ИСО/МЭК 8824-93.

ASN.1 is совместный стандарт ISO, International Electrotechnical Commission International (IEC), и ITU-T (Telecommunication Standardization Sector). Принят в 1984 как часть CCITT X.409:1984. В 1998году заменен на серию X.680.

- Где используются нотации ASN.1:

Basic Encoding Rules (BER), CanonicalEncoding Rules (CER),Distinguished Encoding Rules (DER),XML Encoding Rules (XER),Canonical XML Encoding Rules (CXER),Extended XML Encoding Rules (E-XER),Packed Encoding Rules (PER, unaligned: UPER, canonical: CPER),
Generic String Encoding Rules (GSER),
На уровне приложений:
Application layer protocols such as X.400 electronic mail, X.500 and Lightweight Directory Access Protocol (LDAP) directory services, H.323 (VoIP), Kerberos

# Идентификаторы объектов (Object Identifier (OIDs)
# Дерево идентификаторов объектов(OID-tree)


www.oid-info.com

891,598 OIDs are stored in this repository

**itu-t(0)**
**ITU-T Study Group 17**
[other identifiers: ccitt, itu-r]
child OIDs: recommendation(0) question(1) administration(2) network-operator(3) identified-organization(4) r-recommendation(5) data(9)

**iso(1)ANSI (American National Standards Institute)**
child OIDs: standard(0) registration-authority(1) member-body(2) identified-organization(3)

**joint-iso-itu-t(2)**
[other identifier: joint-iso-ccitt]
ITU-T SG 17 & ISO/IEC JTC 1/SC 6 , 36 child oids
....
Country (16)
....

# Мировой опыт построения дерева идентификаторов объектов на основе серии X.660

**X.660 | ISO/IEC 9834-1 - национальный администратор (Registration Authority).**

– AFNOR (Association Française de Normalisation, the ISO member body for France) - OIDs для Франции под {iso(1) member-body(2) fr(250) type-org(1)};

– ANSI (American National Standards Institute, the ISO member body for the USA) - OIDs для организаций США под {iso(1) member-body(2) us(840) organization(1)};

– BSI (British Standards Institute, the ISO member body for the UK) - OIDs для Великобритнии под {iso(1) member-body(2) uk(826)};

– COSIRA (Canadian Open Systems Interconnection Registration Authority) - OIDs для Канады (Canada) под {joint-iso-itu-t(2) country(16) ca(124)};

– Австралийские компании могут автоматически зарегистрировать OID под {iso(1) member-body(2) au(36)}, основанный на номере компании и бизнес номере (Australian Company Number (ACN) or Australian Business Number (ABN)).

**OID – tree России {iso(1) member-body(2) ru(643) reg1 {1}}**

**OID – tree Украины {joint-iso-itu-t (2) country (16) ua (804) ra (1)}**

# Мировой опыт построения дерева идентификаторов объектов

– ETSI (European Telecommunication Standards Institute) {itu-t(0) identified-organization(4) etsi(0) reserved(127) etsi-identified-organization(0)})
– Операторы сетей используют {itu-t(0) network-operator(3)};
– Телекоммуникационные операторы могут выбрать OID для национальных PTT под {itu-t(0) administration(2)}.
– IANA (Internet Assigned Numbers Authority): OIDs под {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)};
– International allocated OIDs for information systems:
TLS Web server authentication (1.3.6.5.5.7.3);
TLS Web client authentication (1.3.6.5.5.7.3.2);
Signing of downloadable executive code (1.3.6.5.5.7.3.3);
E-mail protection (1.3.6.5.5.7.3.4);
IP Security end system (1.3.6.5.5.7.3.5);
1.3.6.5.5.7.3.6 IP Security tunnel termination
1.3.6.5.5.7.3.7 IP Security user
1.3.6.5.5.7.3.8 Time Stamp Signing

# X.500 — серия стандартов ITU-T (1993 г.) для службы распределенного каталога сети.

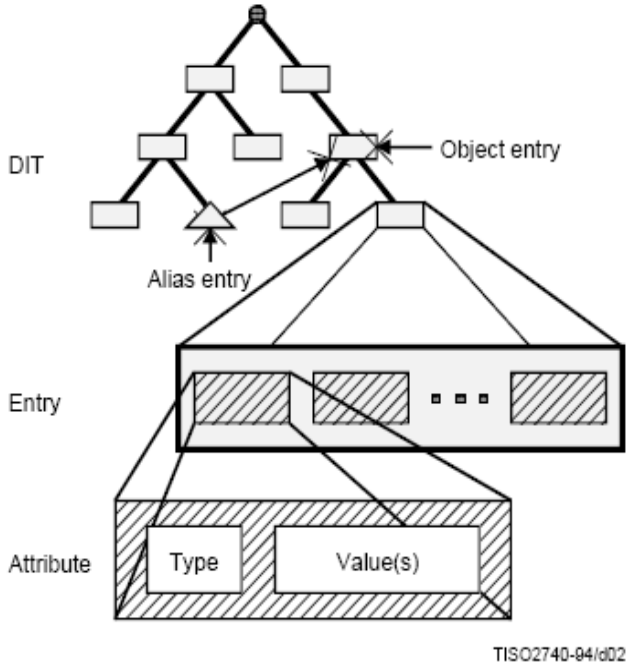



Figure 2 – Structure of the DIT and of Entries

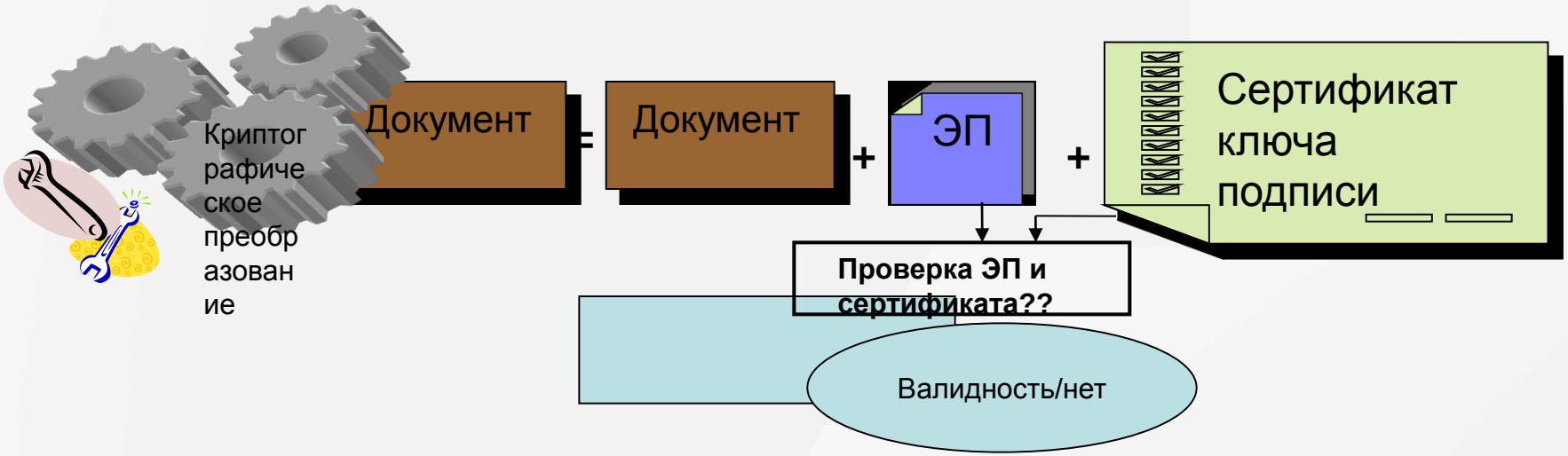
**Международные проекты**
**Challenge и Electronic Color Pages ( Yellow Pages, White Pages, Blue Pages, зеленый Green Pages )**

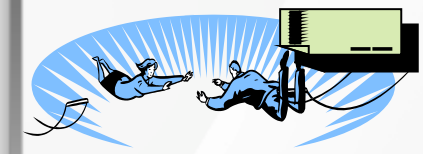
| RDN имя | Объектный класс | Описание |
|---|---|---|
| cn=Joe Bloggs | organizationalPerson<br>OBJECT-CLASS ::= {<br>SUBCLASS OF { person }<br>MAY CONTAIN {<br>LocaleAttributeSet |<br>PostalAttributeSet |<br>TelecommunicationAttributeSet |<br>organizationalUnitName |<br>title }<br>ID id-oc-organizationalPerson }<br><br>**organizationalPerson== 2.5.6.7**<br><br>person OBJECT-CLASS ::= {<br>SUBCLASS OF { top }<br>MUST CONTAIN {<br>commonName \| surname }<br>MAY CONTAIN { description |<br>telephoneNumber |<br>userPassword |<br>seeAlso }<br>ID id-oc-person }<br>**person =2.5.6.6** | Объектный класс Organizational Person (организационная персона) используется для определения записей, которые представляют людей, нанятых данной организацией или имеющих какое-то другое достаточно важное отношение с данной организацией.<br><br>Объектный класс Person (персона) используется для определения записей, которые используются для представления людей в общем виде. |

**Электронная подпись** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для **определения лица,** подписывающего информацию. (Федеральный закон Российской Федерации № 63 от 6 апреля 2011г.).

**Усиленная электронная подпись** – усиленная квалифицированная и усиленная неквалифицированная : криптографическое преобразование информации с использованием ключа электронной подписи, создается с использованием средств ЭП, позволяет определить лицо, подписавшее электронный документ… (ст5 ФЗ № 63).

**Сертификат ключа проверки электронной подписи** – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие **принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи**. (Федеральный закон Российской Федерации № 63 от 6 апреля 2011г.).





**Доверие к ЭП и сертификату?!**
**Структура сертификата определена рекомендацией МСЭ X.509 и RFC 5280, ФЗ № 63 «Об электронной подписи», Приказ ФСБ России № 795**

Копия сертификата ключа подписи (пример)

Сведения о сертификате:
Действителен с 25 октября 2013 г. 7:12:00 UTC по 25 октября 2014 г. 7:17:00 UTC
Версия: 3 (0x2)
Серийный номер: 7A73 876B 0000 0000 2ECA
Издатель сертификата: CN (2.5.4.3) = ООО Русь-Телеком (УЦ РТ1), O (2.5.4.10) = ООО Русь-Телеком, OU (2.5.4.11) = Удостоверяющий центр, STREET (2.5.4.9) = Проезд Маршала Конева дом 29, L (2.5.4.7) = Смоленск, S (2.5.4.8) = 67 Смоленская область, ИНН (1.2.643.3.131.1.1) = 006731071801, ОГРН (1.2.643.100.1) = 1086731015172, C (2.5.4.6) = RU, E (1.2.840.113549.1.9.1) = uc@rus-telecom.ru
Срок действия:
Действителен с: 25 октября 2013 г. 7:12:00 UTC
Действителен по: 25 октября 2014 г. 7:17:00 UTC
Владелец сертификата: ИНН (1.2.643.3.131.1.1) = 006731079110, ОГРН (1.2.643.100.1) = 1106731000309, СНИЛС (1.2.643.100.3) = 07967909XXX, E (1.2.840.113549.1.9.1) = fedotova@garant-telecom.ru, C (2.5.4.6) = RU, S (2.5.4.8) = 67 Смоленская область, L (2.5.4.7) = Смоленск, O (2.5.4.10) = ООО Вега, OU (2.5.4.11) = Руководители, CN (2.5.4.3) = XXXXXXXXX XXXXXXXX XXXXXXXXXXXX, T (2.5.4.12) = Директор
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19

## Предложения

Рассмотреть возможность (по согласованию со странами СНГ):

- разработки документов для описания структуры справочников электронного правительства стран СНГ;

- разработки документов для описания единой структуры веток дерева идентификаторов объектов электронных правительств стран СНГ

# Спасибо за внимание!

Игнатьева Марина Алексеевна

ignatm90@mail.ru