The Use of Electronic Signature in Processes and Applications of the Croatian Agency for Medicinal Products and Medical Devices

Arian Rajh, Dubravka Sudic, Katarina Gvozdanovic
Agency for Medicinal Products and Medical Devices
Zagreb, Croatia
e-mail: arajh@halmed.hr, dsudic@halmed.hr, kgvozdanovic@halmed.hr

***Abstract*—In this paper, we describe the Information Technology (IT) solution for electronic signature in the Agency for Medicinal Products and Medical Devices of Croatia (HALMED). Electronic signature with various certificates is currently enabled in the Windows setting and tested across HALMED's Digital Archival Information System. HALMED's plans include the digital transformation of the main processes.**

Keywords—digital transformation; Digital Signature Services; electronic signature; eSignature building block; paperless agency; Qualified Electronic Signature; Digital Archival Information System.

I. INTRODUCTION

The European Telecommunications Standards Institute (ETSI) explains electronic (digital) signature as "essentially the equivalent of a hand-written signature, with data in electronic form being attached to other electronic subject data (Invoice, Payment slip, Contract, etc.) as a means of authentication" [1]. EU Regulation on Electronic Identification and Trust Services (EU Regulation 910/2014 of 23 July 2014, eIDAS) states that an electronic signature is "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign" [2].

eIDAS differentiates electronic signatures, Advanced Electronic Signatures (AES), and Qualified Electronic Signatures (QES). An Advanced Electronic Signature is used under control of the signatory, it identifies the signatory, and it is associated with the signatory without any uncertainty. It can be used to show if the signed content has been changed. A Qualified Electronic Signature creation device creates a QES, which can legally replace a handwritten signature. All EU countries should recognize QES based on a qualified certificate and issued by a qualified trust service provider. The provider should be listed on the European Trusted List [3]. A qualified certificate for electronic signatures holds data that clearly represents the qualified trust service provider and the natural or legal person. An electronic record signed with QES should not require supplementary evidence in courts. This represents a giant step forward for using electronically signed records and working paperless in the EU. EU has also launched an eSignature building block through its Connecting Europe Facility (CEF) instrument to facilitate the use of electronic signature [4]. eSignature building block helps IT-solution providers to develop their solutions in conformance with eIDAS regulation. ETSI provides a free online tool for electronic signature conformance verification [5].

The Agency for Medicinal Products and Medical Devices (HALMED) is the Croatian authority in charge of the regulation and services related to medicinal products, medical devices, homeopathic medicinal products, and veterinary medicinal products. HALMED is responsible for permitting marketing authorizations for the registration of medicinal products and homeopathic medicinal products, for parallel imports of medicinal products, for granting authorizations for manufacturers of medicinal products, for granting authorizations for wholesale distribution of medicinal products, for brokering of medicinal products, and for the retail sale of medical devices. HALMED performs laboratory analyses of medical devices and quality control procedures for medicinal products and homeopathic medicinal products as the official laboratory for the Republic of Croatia. It is responsible for the inspection of the production of active substances, excipients, and finished medicinal products. It approves the entry and import of medicinal products. It monitors adverse reactions in clinical trials and on the marketed products, and conducts pharmacovigilance of medicinal products and vigilance of medical devices. HALMED also advises marketing authorization holders, the Minister of Health, and the public, and cooperates with other EU and international medical agencies within its scope of work as well [6].

In Section II of this paper, we describe processes with electronic signatures in HALMED. In Section III, we discuss the solution and standards that it uses, from both practical and scientific viewpoint. Further work and conclusion are provided in Sections IV and V.

II. PROCESSES IN HALMED WITH ELECTRONIC SIGNATURES

For the time being, HALMED has implemented a general signing procedure with electronic signatures. That means that any record can be signed in its Windows environment as long as it is saved in PDF form (as shown in Fig. 1).

The solution for signing records enables HALMED's employees to verify signatures and signed records. This is the standard function of eSignature software solutions [7]. The next upgrade of this solution should enable the electronic signing of any record in MS Word or PDF directly from HALMED's Digital Archival Information System's (DAIS) environment. This functionality is in the early testing phase. DAIS should automatically convert MS Word records to PDFs before signing. The solution is currently used with

 ISBN: 978-1-61208-763-4

internal certificates, issued by HALMED's organization to its employees, but it can work with any certificate for qualified electronic signatures. The solution was tested with several Croatian trusted certificates. However, to work paperless, HALMED should digitally transform its processes.

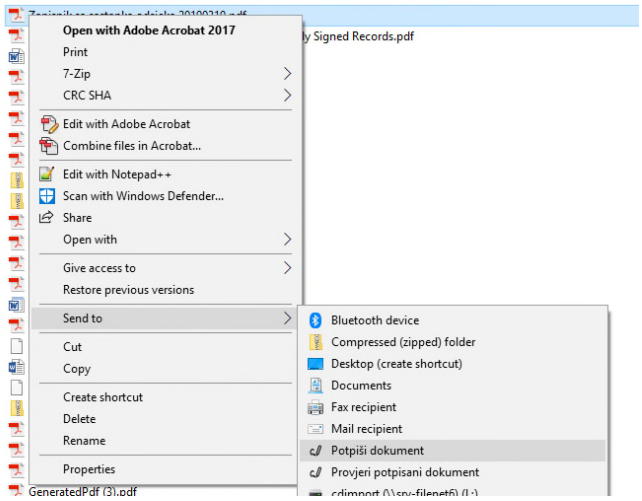

Figure 1. The process of signing records in the Windows environment.

Next, we describe and explain the IT solution for electronic signatures installed in HALMED more closely.

III. Solution For Signing with Electronic Signature Implemented in Halmed

The IT solution for electronic signatures in HALMED was developed and provided by Ericsson Nikola Tesla company (ENT, www.ericsson.hr). ENT has been working closely with HALMED on various occasions. This IT company won the EU-financed project of developing HALMED's DAIS in 2013. This IT solution for signing electronic records represents a logical upgrade of DAIS. The signing solution was based on CEF eSignature building block to ensure its compatibility with eIDAS regulation and to decrease the level of legal risk in HALMED's work with electronically signed records.

CEF eSignature building block was provided to assist "public administrators and businesses to accelerate the creation and verification of electronic signatures" [8]. The eSignature building block was established upon the following standards [9]-[13]:

- ETSI EN 319 132 XML Advanced Electronic Signatures (XAdES)
- ETSI EN 319 122 CMS Advanced Electronic Signatures (CAdES)
- ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES)
- ETSI EN 319 162 Associated Signature Containers (ASiC)
- ETSI TS 119 612 v2.1.1 Electronic Signatures and Infrastructures (ESI), Trusted Lists

The building block includes Digital Signature Services (DSS), open-source software for the creation and validation of eIDAS-conformant electronic signatures. IT-solution providers can use DSS according to the GNU Lesser General Public Licence 2.1. The current DSS version is 5.5 [14].

The IT solution for signing electronic records works with certificates compatible with RFC 5280 and X509 standard, RFC 7292 and PKCS#12/Personal Exchange File (PFX) standards [15]- [16]. The procedural and technological basis for working with electronic signature is Public Key Infrastructure (PKI). PKI connects public keys with natural or legal subjects via registration procedure. X509 is a standard that determines public key certificates and revocation lists. PKCS#12 is used for the binding of various cryptography objects, like private keys and certificates, to a file.

The IT solution for electronic signatures enables using internal or other certificates, e.g., certificates issued by a trusted service, as well as choosing a business role or a reason for signing an electronic record [17]. This is the first advantage of the solution; it can work with various certificates. Certificates should be compatible with X509, RFC 5280, PKCS#12 and PFX standards. The solution in its web-part uses RFC 8446 Transport Layer Security (TLS) cryptographic protocol for safe communication over the internet [18]. The solution also contains its local installation. As the web part of the solution communicates with the service installed locally, the TLS certificate should be issued for the localhost domain. The solution adds the table with data about signing and the signer at the end of the records. A property file contains definitions of signatories' roles, and an administrator in HALMED can change this file. The table contains the following data: signatory, role, date, time, and time zone.

DAIS is a wide-range IT system and HALMED's digital archives, developed by ENT for HALMED under the EU-financed project in 2013 and 2014. It was established on the IBM FileNet platform, and it contains several modules. The basic module is Content Navigator; it enables working with any electronic records and starting various record-driven processes (see Fig. 2 that shows the folder view and organization in HALMED's DAIS, and the folder in the example contains action plans and analyses records).

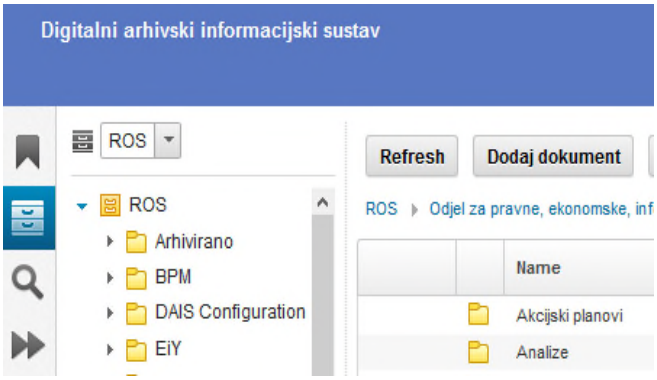

Figure 2. Content Navigator.

 ISBN: 978-1-61208-763-4

The second module is Enterprize Records. Enterprize Records is a records management and archival management module, and it is connected with HALMED's archival (metadata) management system Pismohrana (the Archive). IT Company Omega-Software developed Pismohrana in 2012 (www.omega-software.hr). It is a process-driven application based on professional standards of the International Council of Archives (www.ica.org/en). The purpose of the DAIS Enterprize Records module is to capture archival metadata from Pismohrana application and protect the records, or to execute an activity upon the records, triggered by Pismohrana application. Enterprize Records module works with EMC2 (from the names of the IT company founders Egan, Marino, Conolly, and Curly) Isilon archival storage and moves archived records from active HP 3PAR storage to slower, but more protected Isilon storage. DAIS also works with an integrated PDF/A file converter.

The third module is a module for ingest of ISO 14721-compatible [19] submitted packages with records and their metadata into the DAIS repository (see Fig. 3 that shows the analysis, migration and export of packages functions). By using this module, records are prepared for description in Pismohrana application and transported into the DAIS repository, and their metadata are transferred and linked to newly-established digital objects in the repository. Metadata are used for the retrieval and management of archived records.

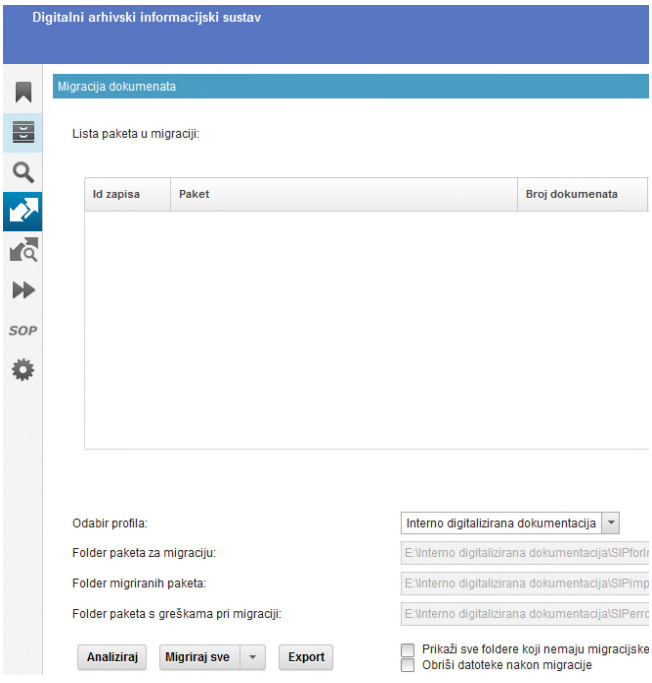

Figure 3. The migration module.

The fourth module is related to business processes and management of workflows. The next module is a module related to the creation and management of HALMED's Quality Management System. This module enables the role-defined creation of Standard Operative Procedure (SOP) records and related templates and reports. It notifies SOP authors and their managers when an SOP needs to be reviewed and updated and enables automated distribution and archiving of new versions upon their completion. HALMED's employees are signing new SOPs by using the previously developed functionality of signing electronic records. This functionality works with the same internal certificates. The difference is related to the visual appearance of the table with signatures and the fact that it is placed at the beginning of the record (see Fig. 4 and 5 - Fig. shows the header of SOP records' template).

AGENCIJA ZA LIJEKOVE I MEDICINSKE PROIZVODE		
NASLOV:		

Figure 4. Table for signatures in an SOP record.

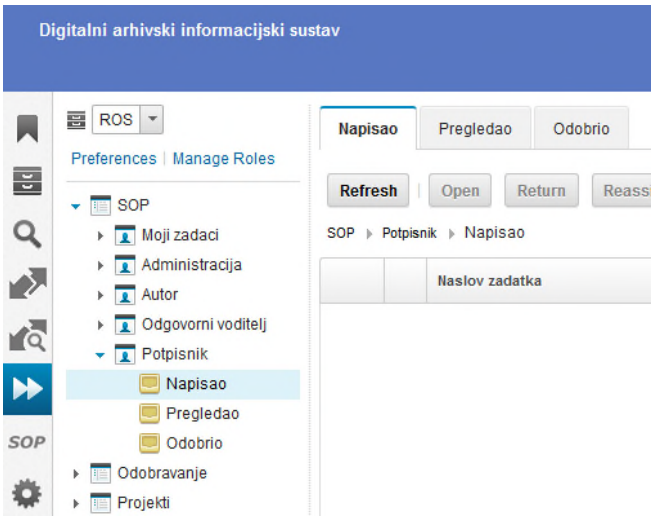

Figure 5. The role-dependent signing of SOP records in the Quality Management module, by using integrated functionality for signing electronic records.

The next module is used for the administration of HALMED's internal projects, like the development and customizations of business applications, digitization, and other projects. The signing function is not integrated with this module, but HALMED has developed plans to enable electronic signatures in this module in the next few years. In this time, HALMED's project managers and the members of the groups for the supervision of HALMED's projects use the signing functionality in the Windows environment, as shown in Fig. 1. Finally, there is a module for the administration of the DAIS system and its users.

IV. FURTHER WORK

The near phase of development of HALMED's options with electronic signatures comes down to the implementation

 ISBN: 978-1-61208-763-4

of electronic signature across the DAIS environment, i.e., across all modules except the admin module. The ability to use the solution across at least two different environments is the second advantage. Various business applications (for approval of medicines, for medical devices, for inspections) connect with DAIS, so the solution should automatically facilitate electronic signatures in these specific business environments.

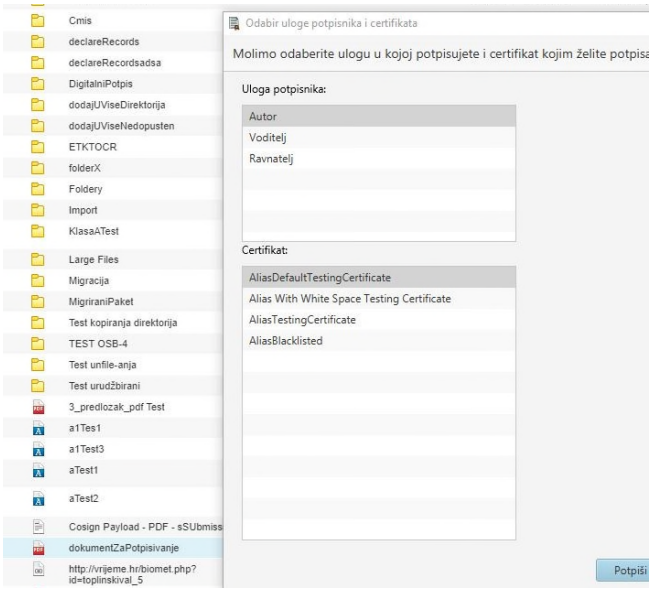

Figure 6. Signing of an electronic record in the DAIS pre-production environment (figure taken from the functional specification).

Ericsson Nikola Tesla developed this functionality of signing in DAIS for HALMED, and currently, it is in the testing phase. Fig. 6, taken from Ericsson Tesla's functional specification, shows the selection of record, signer's role, and a certificate from the list of available certificates. Fig. 7 shows the saving of electronically signed records as the main version in the DAIS repository. However, solely the implementation of electronic signature across the entire DAIS system will not enable HALMED to work paperless.

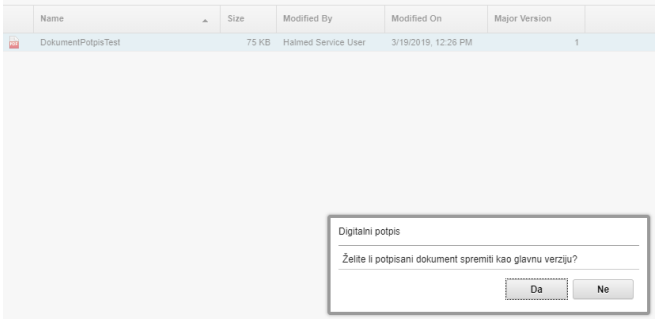

Figure 7. Saving the electronically signed record as the new main version, a figure from the functional specification.

The plans for further development include business process reengineering for main HALMED's business processes, starting with granting marketing authorization for medicinal products. For this reason, HALMED has gathered a group dedicated to turning the marketing authorization process more comfortable for its clients and its employees. The final goal is to make this process completely paperless. The components of the digital transformation of HALMED's marketing authorization process are the following:

- Reengineering of the business process. The re-engineered and streamlined marketing authorization process should be established upon new activities with electronic records and resources, and these activities cannot "mimic" the existing paper-based process.
- HALMED representatives with process-significant roles should be equipped with legally valid certificates.
- Marketing authorization holders (as HALMED's clients) need to be prepared for the new processes. For this reason, HALMED works on establishing a registration procedure and portal for its clients. Further guidelines should be produced for the clients in the next period.
- Supportive resources should also exist in electronic form. This has already been ensured on the EU-level as the dossiers for medicinal products are being created and transferred to medicines agencies in the electronic Common Technical Document (eCTD) format [20]. HALMED has actively participated in this EU initiative since 2008, it has enabled work with electronic eCTD resources since 2010 on the national level, and since 2013 on the EU level.
- DAIS should enable archiving the electronically signed records. Additional customization of DAIS was planned for the 2020/2021 period. The debate is run on possible utilization of blockchain and distributed ledger technologies for ensuring the information on the authenticity of electronically signed records in a particular period [21] [22].

Another example of the digital transformation of the business process, which occurs in HALMED right now, is the reengineering of the support process related to employee vacations. For this reason, HALMED has initiated the customization of its ERP and HR (Human Resources) system (developed by the local company Irata, www.irata.hr). This process will also use electronically signed records.

V. CONCLUSION

HALMED has taken the preliminary step when enabling the functionality of electronic signing. The solution is based on the CEF eSignature building block, it is compatible with EU practice, and it works with various certificates. The innovative application of relevant standards and the usability

on Windows and FileNet primary platforms, as well as on HALMED's business platforms, represent both the scientific and practical contribution to the electronic signature subject matter. After the digital transformation of the marketing authorization process, what HALMED is currently solving, other core and support processes will follow. Establishing the generic process of signing electronic records is not sufficient for the successful functioning of a paperless organization – the complete digital transformation of selected business processes should be performed. In this sense, technology can assist the digital transformation of an organization, but the actual work on the processes cannot be dodged.

ACKNOWLEDGMENT

The authors have presented the case implemented at the Agency for Medicinal Products and Medical Devices of Croatia (HALMED); hence, HALMED has funded the project and, therefore, contributed to this research.

REFERENCES

[1] "Digital Signature," n.d., URL: https://www.etsi.org/technologies/digital-signature [retrieved: February, 2020].

[2] EU Regulation 910/2014 of 23 July 2014 (eIDAS), URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EE#d1e2373-73-1 [retrieved: February, 2020].

[3] "Trusted List Browser," 2019, URL: https://webgate.ec.europa.eu/tl-browser/# [retrieved: February, 2020].

[4] "Introduction to the Connecting Europe Facility. eSignature building block," 2016, URL: https://www.esens.eu/sites/default/files/building_block_dsi_introdocument_esignature_v0.0.20_3.pdf [retrieved: February, 2020].

[5] "ETSI Signature Conformance," n.d., URL: https://signatures-conformance-checker.etsi.org/pub/index.shtml [retrieved: February, 2020].

[6] "HALMED Activities," 2019, URL: http://www.halmed.hr/en/O-HALMED-u/Osnovni-podaci-i-dokumenti/Djelatnosti/ [retrieved: February, 2020].

[7] C. Kościelny, "An Electronic Signature and Hash Functions," Springer, Berlin, Heidelberg, 2013, chapter 5, pp. 127-145, in Kościelny, C., Kurkowski, M., and Srebrny, M., Modern Cryptography Primer, ISBN: 978-3-642-41386-5.

[8] "CEF Digital About. Definitions," n.d., URL: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions#CEFDefinitions-eSignatureDefinitions [retrieved: February, 2020].

[9] ETSI EN 319 132 XML Advanced Electronic Signatures (XAdES). URL: https://www.etsi.org/deliver/etsi_en/319100_319199/3191320 1/ and https://www.etsi.org/deliver/etsi_en/319100_319199/3191320 2/ [retrieved: February, 2020].

[10] ETSI EN 319 122 CMS Advanced Electronic Signatures (CAdES). URL: https://www.etsi.org/deliver/etsi_en/319100_319199/3191320 1/ and https://www.etsi.org/deliver/etsi_en/319100_319199/3191220 1/ [retrieved: February, 2020].

[11] ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES). URL: https://www.etsi.org/deliver/etsi_en/319100_319199/3191420 1/ and https://www.etsi.org/deliver/etsi_en/319100_319199/3191420 2/ [retrieved: February, 2020].

[12] ETSI EN 319 162 Associated Signature Containers (ASiC). URL: https://www.etsi.org/deliver/etsi_en/319100_319199/3191620 1/ and https://www.etsi.org/deliver/etsi_en/319100_319199/3191620 2/ [retrieved: February, 2020].

[13] ETSI TS 119 612 v2.1.1 Electronic Signatures and Infrastructures (ESI), Trusted Lists. URL: https://www.etsi.org/deliver/etsi_TS/119600_119699/119612/02.01.01_60/ts_119612v020101p.pdf [retrieved: February, 2020].

[14] "Digital Signature Services (DSS). The current release," 2019, URL: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS [retrieved: February, 2020].

[15] "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," n.d., URL: https://tools.ietf.org/html/rfc5280#section-4.2.1.9 [retrieved: February, 2020].

[16] K. Moriarty, M. Nystrom, S. Parkinson, A. Rusch, and M. Scott, "PKCS#12: Personal Information Exchange Syntax v.1.1.," 2014, URL: https://tools.ietf.org/html/rfc7292 [retrieved: February, 2020].

[17] Ericsson Nikola Tesla, "FS01 Nadogradnja funkcionalnosti potpisivanja dokumenta. Funkcionalna specifikacija (FS01 Customization of the function of signing records. Functional specification)," 2019, unpublished (technical document of the software upgrade project).

[18] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3.," 2018, URL: https://tools.ietf.org/html/rfc8446 [retrieved: February, 2020].

[19] ISO 14721:2012. Space data and information transfer systems – Open archival information system (OAIS) – Reference Model (reviewed and confirmed in 2018). URL: https://www.iso.org/standard/57284.html [retrieved: February, 2020].

[20] "eCTD," 2019, *URL*: http://esubmission.ema.europa.eu/eCTD%20NMV/eCTD.html [retrieved: February, 2020].

[21] "Work program of the ISO/TC 307 Blockchain and distributed ledger technologies technical committee," n.d., URL: https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0 [retrieved: February, 2020].

[22] V. L. Lemieux, "A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation," in Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, Dec. 2017, pp. 2271-2278, doi: 10.1109/BigData.2017.8258180

 ISBN: 978-1-61208-763-4