INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

# Efektivitas dan Kelemahan Autentikasi Berbasis Web Menggunakan One-Time Password (OTP) dalam Mencegah Akses Tidak Sah

**Fajar Maulana[1], Yomei Hendra[2], Putri Sakinah[3], Yofhanda Septi Eirlangga[4], Aisyah Qurrata Ayun[5]**

[1,2,3,4,5]Infomatika, Universitas Adzkia

Email : fajar@adzkia.ac.id[1], yomei@adzkia.ac.id[2], putri@adzkia.ac.id[3], yofhanda@adzkia.ac.id[4], aisyah@adzkia.ac.id[5]

*Corresponding Author :* fajar@adzkia.ac.id

***Abstract***

*Authentication based on one-Time Password (OTP) is one method that is widely used in securing access to web systems. This study aims to analyze in depth the effectiveness and weaknesses of the OTP authentication system in preventing unauthorized access. Through a qualitative approach based on literature studies, as well as comparisons between other authentication methods, it was found that OTP is able to increase a significant additional layer of security, especially when combined with other authentication methods such as passwords or biometrics. However, this system still has various weaknesses, such as the risk of phishing attacks, man-in-the-middle (MITM) attacks, and vulnerabilities to SIM swapping attacks, especially in the implementation of OTP via SMS. Dependence on user devices and communication networks is also a limiting factor in the effectiveness of OTP. This study provides recommendations for the implementation of strengthening measures such as Multi-Factor Authentication (MFA), the use of authenticator applications, and the implementation of end-to-end encryption to reduce security risks. The results of this study are expected to be a reference for system developers and organizations in choosing and implementing authentication methods that are more secure and in accordance with current cybersecurity needs.*

***Keywords :*** *OTP, Web Authentication, cybersecurity, unauthorized access, Multi-Factor Authentication, Phishing, MITM.*

## I. Pendahuluan

Perkembangan teknologi digital dan internet telah meningkatkan risiko terhadap keamanan informasi, terutama pada sistem dan layanan berbasis web yang rentan terhadap serangan siber. Masalah utama yang dihadapi adalah mencegah akses tidak sah ke data sensitif, dengan ancaman seperti pencurian kata sandi, phishing, dan serangan *brute-force* yang dapat menyebabkan kerugian finansial dan reputasi. Autentikasi memainkan peran krusial dalam melindungi akses ke sistem. Metode autentikasi tradisional berbasis kata sandi statis sering

INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

dianggap tidak memadai karena mudah ditebak atau dicuri. Untuk meningkatkan keamanan, banyak organisasi beralih ke metode autentikasi lebih canggih seperti One-Time Password (OTP). OTP memberikan kata sandi sekali pakai yang hanya berlaku untuk satu sesi atau transaksi, dan sering digunakan sebagai bagian dari autentikasi dua faktor (2FA) untuk menambah lapisan keamanan. Meskipun OTP meningkatkan keamanan, metode ini memiliki kelemahan seperti kerentanan terhadap serangan Man-in-the-Middle (MitM), phishing, dan ketergantungan pada jaringan telekomunikasi yang tidak selalu andal. Selain itu, penggunaan OTP yang berulang dapat menyebabkan ketidaknyamanan bagi pengguna, yang mungkin mengurangi efektivitasnya. Untuk mengevaluasi efektivitas dan kelemahan OTP, kami menyajikan diagram alur penelitian berikut. Diagram ini menggambarkan tahapan penelitian dari perencanaan hingga analisis hasil, memberikan gambaran jelas tentang langkah-langkah yang diambil dan kontribusi setiap tahap dalam mencapai tujuan penelitian. Dengan diagram ini, diharapkan pembaca dapat memahami proses penelitian secara menyeluruh.

## II. Landasan Teori

### Autentikasi

Autentikasi adalah suatu metode untuk menentukan atau memastikan bahwa seseorang (atau sesuatu) adalah asli atau benar. Adapun proses validasi user pada saat memasuki sistem yaitu nama dan password dari user melalui proses pengecekan user pada suatu database yang diregistrasi sebelumnya oleh user itu sendiri. Pada sistem komputer, autentikasi biasanya terjadi pada saat login atau permintaan akses.

Selain itu autentikasi juga merupakan salah satu dari banyak metode yang digunakan untuk membuktikan bahwa dokumen tertentu yang diterima secara elektronik asli datang dari orang yang bersangkutan dan tidak berubah keasliannya, dengan cara mengirimkan suatu kode tertentu melaui e-mail kemudian pemilik e-mail membalas e-mail tersebut.

Autentikasi server berfungsi untuk mengenali user yang berintegrasi ke jaringan dan memuat semua informasi dari user tersebut. Dalam praktek biasanya autentikasi server mempunyai database dengan fungsi untuk menjaga server jika suatu saat ada masalah, segala informasi di dalamnya tidak akan terganggu.

### *One Time Password* (OTP)

Tujuan dari pembuatan OTP (password sekali pakai) adalah untuk mempersulit pihak-pihak yang tidak bertanggung jawab dalam mengakses data yang rahasia. Seperti account komputer. Biasanya password statis lebih mudah untuk diakses pihak-pihak yang tidak bertanggung jawab, cukup dengan adanya usaha dan waktu. Dengan secara konstan merubah password setiap kali penggunaanya, maka resiko password diketahui pihak lain dapat dikurangi.

## III. Metode Penelitian

INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

Penelitian ini dirancang menggunakan pendekatan deskriptif kualitatif berbasis studi literatur dan analisis komparatif, yang bertujuan untuk mengidentifikasi, mengevaluasi, dan membandingkan efektivitas dan kelemahan autentikasi berbasis One-Time Password (OTP) dalam mencegah akses tidak sah pada sistem web. Model ini dipilih karena memungkinkan peneliti untuk menggali data sekunder secara mendalam dari berbagai sumber kredibel seperti jurnal ilmiah, laporan industri, dokumentasi teknis, dan kasus nyata yang relevan dengan praktik OTP.

**Jenis dan Pendekatan Penelitian**

Jenis penelitian ini bersifat deskriptif karena bertujuan untuk menggambarkan fenomena yang terjadi di lapangan dan menjelaskan variabel serta hubungan antar variabel secara sistematis. Pendekatan kualitatif digunakan karena data yang diperoleh bersifat non-numerik, lebih menekankan pada pemahaman, interpretasi, serta evaluasi fenomena keamanan OTP dari sudut pandang praktis dan teoritis.

**Efektivitas**

Efektivitas merujuk pada seberapa baik suatu sistem mencapai tujuannya. Dalam konteks ini, artinya seberapa berhasil OTP dalam mencegah akses tidak sah ke sistem web.

**Aspek yang dinilai:**

1. Kemampuan OTP menambah lapisan keamanan setelah username & password.
2. Penurunan tingkat keberhasilan serangan brute force atau credential stuffing.
3. Kepuasan pengguna (usability) saat menggunakan sistem OTP.

**Kelemahan**

Kelemahan menunjukkan sisi rawan dari sistem OTP. Meskipun OTP meningkatkan keamanan, ia tidak sepenuhnya kebal terhadap serangan, seperti:

1. Phishing: OTP bisa dicuri lewat situs palsu.
2. Man-in-the-Middle (MitM): OTP bisa dicegat saat dikirimkan lewat jaringan publik.
3. SIM Swap Attack: Penyerang memindahkan nomor korban ke SIM palsu.
4. Delay / Expiry: SMS OTP kadang terlambat atau gagal dikirim.

**Autentikasi Berbasis Web**

Autentikasi berbasis web adalah proses verifikasi identitas pengguna melalui aplikasi atau situs web. Biasanya dilakukan dengan mengakses halaman login dan mengisi kredensial (username, password), lalu menggunakan OTP sebagai verifikasi tambahan.

**Menggunakan *One-Time Password* (OTP)**

*One time password* (OTP) merupakan sebuah kode yang digunakan hanya sekali untuk otentiasi pengguna dalam sebuah sesi. Kode ini dihasilkan secara unik dan tidak dapat

INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

digunakan Kembali, sehingga memberikan tingkat keamanan yang lebih tinggi dalam melawan serangan seperti serangan replay. One-Time Password (OTP) adalah kode sandi yang hanya berlaku sekali pakai dan memiliki masa berlaku yang sangat singkat. OTP biasanya digunakan sebagai lapisan keamanan tambahan dalam proses autentikasi, khususnya dalam sistem Two-Factor Authentication (2FA). Kode ini biasanya dikirimkan melalui SMS, email, atau aplikasi autentikator (seperti Google Authenticator atau Authy) setelah pengguna memasukkan username dan password.

**Dalam Mencegah Akses Tidak Sah**

Tujuan utama OTP adalah mengurangi risiko penyusup yang berhasil masuk menggunakan kredensial curian. OTP menjadi lapisan pertahanan kedua setelah password (Two-Factor Authentication – 2FA). Namun, efektivitas ini bergantung pada: Media pengiriman OTP (SMS < App-based),Edukasi pengguna agar tidak mudah tertipu phishing, Kombinasi dengan metode lain seperti biometrik atau CAPTCHA.


**Gambar 1 Efektivitas dan Kelemahan Autentikasi Berbasis Web Menggunakan *One-Time Password* (OTP)**

## IV. Hasil Dan Pembahasan

Untuk mengetahui hasil dari analisis sentimen ulasan Efektivitas Dan Kelemahan Autentikasi Berbasis Web Menggunakan *One-Time Password* (OTP) Dalam Mencegah Akses Tidak Sah , beikut adalah langkah-langkah yang peneliti terapkan menggunakan Google kodular denganaplikas pendukung OTP yaitu Firebase.

**Prosedur Penelitian**

Penelitian ini dilaksanakan melalui tahapan-tahapan sebagai berikut:

| Tahap | Uraian |
|---|---|
| Identifikasi Masalah | Merumuskan persoalan utama tentang efektivitas dan kelemahan OTP dalam konteks web security |
| Kajian Literatur | Mengumpulkan dan mereview literatur terkini mengenai sistem OTP dan teknologi autentikasi lainnya |
| Analisis Implementasi | Menelaah model OTP seperti TOTP, HOTP, SMS OTP, dan App-based OTP dari sisi teknis dan keamanannya |
| Analisis Komparatif | Membandingkan OTP dengan metode autentikasi lain seperti biometrik, passwordless, dan passkeys |
| Identifikasi Kelemahan | Menyusun klasifikasi kerentanan berdasarkan kasus nyata seperti phishing, SIM swap, intercept OTP |
| Penyusunan Rekomendasi | Merancang strategi keamanan berdasarkan best practice seperti MFA, enkripsi E2E, dan edukasi pengguna |
| Penyusunan Laporan | Merangkum seluruh hasil penelitian ke dalam dokumen ilmiah untuk keperluan akademik dan praktis. |

**Teknik Analisis Data**

Data dianalisis menggunakan teknik:

1. Analisis Isi (Content Analysis): Digunakan untuk meninjau isi literatur secara sistematis, mengidentifikasi tren, pola, dan hasil penelitian sebelumnya terkait OTP dan autentikasi web.
2. Analisis Tematik (Thematic Analysis):

INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

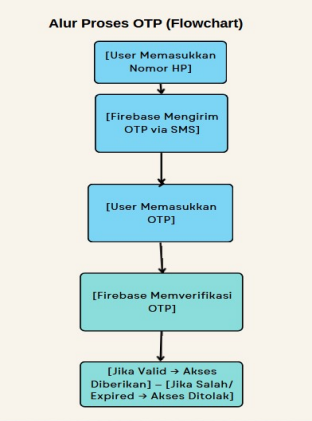
Teknik ini digunakan untuk mengelompokkan data ke dalam tema-tema utama seperti bentuk serangan, mitigasi risiko, efisiensi OTP, dan perbandingan metode autentikasi.

3. Analisis Komparatif:
   Digunakan untuk membandingkan antara OTP dan metode autentikasi lainnya dari segi keamanan, kemudahan, dan ketergantungan perangkat. Tabel komparatif digunakan untuk memperjelas hasil analisis ini.
4. Analisis SWOT (Strengths, Weaknesses, Opportunities, Threats):
   Teknik ini digunakan untuk mengidentifikasi kekuatan dan kelemahan OTP, serta peluang dan tantangan yang dihadapi dalam implementasi sistem autentikasi modern.

**Alur Flow Chart OTP**

**Flowchart proses login dengan OTP untuk autentikasi berbasis web**

Flowchart ini menggambarkan alur umum pengguna melakukan login dengan sistem OTP (baik berbasis SMS atau aplikasi seperti Google *Authenticator*):




**Gambar 2. Alur Flow Chart OTP**

Penjelasan:

1. User Akses Login: Pengguna mengakses halaman login.
2. Input Username & Password: Input awal sebelum autentikasi dua langkah.
3. Validasi Kredensial Awal: Mengecek apakah username dan password sesuai.
4. Sistem Kirim OTP: OTP dikirimkan melalui media yang telah ditentukan (SMS/email/aplikasi).
5. Input OTP: Pengguna mengisi kode OTP yang diterima.
6. Validasi OTP: Sistem mencocokkan OTP dengan yang dikirim.
7. Akses Diberikan / Error: Jika OTP valid, akses diberikan; jika salah, pengguna diberi notifikasi.

**Pengujian Program**

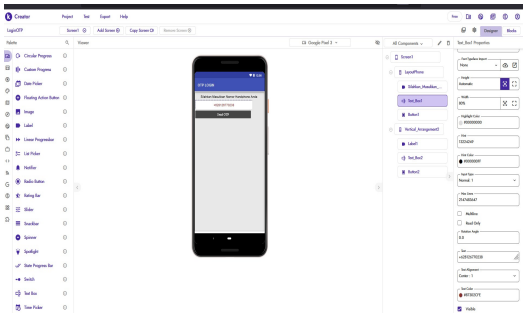
Penguji mengujikan program dengan menggunakan aplikasi kodular dengan Firebase Login dengan OTP (One Time Password) di Kodular

INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

dengan menggunakan no hp untuk menjalankan aplikasi kodular. Penulis juga menggunakan mobile programing yang di sponsori oleh google dengan aplikasi pembantu yaitu firebase. cara kerja sistem *One-time-Password* pada program ini adalah pengguna dapat memasukkan no handphone dan kode OTP yang diperlukan untuk verifikasi OTP.

Implementasi sistem verifikasi login menggunakan OTP melalui No HP telah berhasil dilakukan. Sistem ini terdiri dari beberapa komponen Utama yaitu backed server dari firebase, No Hape sebagai API, dan antar muka pengguna Backend server dikembangkan menggunakan Google Firebase adalah platform pengembangan aplikasi yang disediakan oleh Google untuk membantu developer membangun, mengelola, dan menskalakan aplikasi web maupun mobile secara efisien. Firebase menyediakan berbagai layanan backend tanpa perlu membangun server sendiri, sehingga sangat cocok untuk pengembangan cepat dan integrasi berbagai fitur modern.

Fungsi Utama Firebase adalah sebagai Autentikasi (Firebase Authentication) dan penyediakan layanan login menggunakan email, password, nomor HP (OTP), Google, Facebook, dll. Cocok untuk implementasi OTP berbasis SMS dengan keamanan tambahan.



**Gambar 3. Memasukkan No Handphone pada Form OTP**

Penelitian ini dilengkapi dengan pengembangan aplikasi autentikasi OTP menggunakan platform Kodular, yang mengilustrasikan bagaimana OTP dikirim dan diverifikasi untuk mengamankan akses pengguna ke sistem.

Berdasarkan Hasil Implementasi Aplikasi memiliki dua fitur utama yaitu Pengiriman OTP via SMS ke nomor HP yang dimasukkan pengguna lalu kode Verifikasi OTP yang dimasukkan oleh pengguna. Aplikasi memanfaatkan layanan pihak ketiga (misalnya Firebase) sebagai backend pengiriman dan verifikasi OTP.

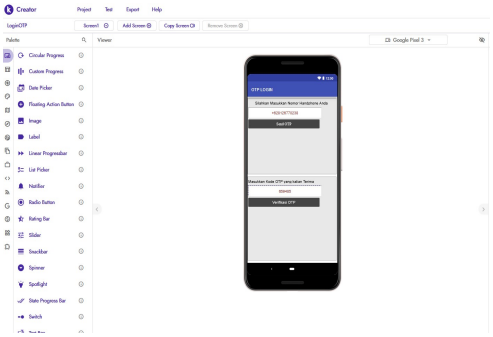
Pada Tampilan Aplikasi (berdasarkan gambar 4):

1. Input Nomor HP: pengguna mengisi nomor ponsel aktif.
2. Tombol "Send OTP": mengirim kode OTP ke nomor tersebut.
3. Input OTP: pengguna memasukkan kode OTP yang diterima.
4. Tombol "Verifikasi OTP": memverifikasi apakah OTP valid atau tidak.

Efektivitas OTP berhasil menambahkan lapisan keamanan ekstra pada proses login pengguna.

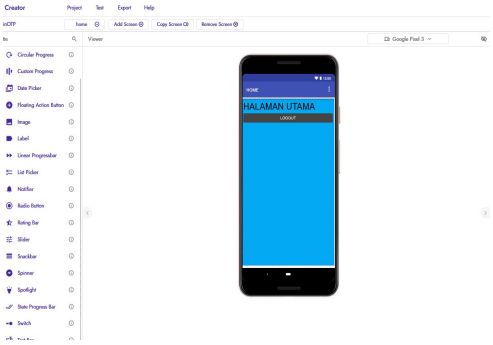
INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

Implementasi OTP mencegah login hanya dengan password atau informasi dasar pengguna, sehingga mengurangi risiko penyalahgunaan akun.
Penggunaan Firebase atau layanan SMS OTP mempercepat proses integrasi tanpa perlu membuat sistem backend sendiri.



**Gambar 4. Proses Verifikasi OTP**

Pada "HALAMAN UTAMA" ditampilkan sebagai indikasi bahwa pengguna telah berhasil masuk, dan Terdapat tombol "LOGOUT", yang menandakan pengguna bisa keluar dari sesi login-nya.




**Gambar 5. Halaman Utama Setelah berhasil Login**

Pada aplikasi menunjukkan bahwa OTP berhasil diverifikasi → pengguna diarahkan ke halaman utama aplikasi. Halaman ini menandai akses telah diberikan secara sah setelah proses autentikasi OTP. Sistem OTP berfungsi secara end-to-end. Verifikasi berhasil mengarah ke halaman utama, sebagai tanda bahwa pengguna telah lolos otentikasi. Aplikasi ini telah menerapkan mekanisme login yang aman, dengan pemisahan antara: Layar berhasil verfikasi OTP dan Layar Akses Utama (Home Page)

## V. Kesimpulan

Berikut adalah kesimpulan dari penelitian " Efektivitas dan Kelemahan Autentikasi Berbasis Web Menggunakan One-Time Password (OTP) dalam Mencegah Akses Tidak Sah":

1. Simulasi menunjukkan bahwa OTP efektif mencegah akses tidak sah jika diimplementasikan dengan benar dan didukung infrastruktur yang aman. Namun, OTP berbasis SMS tetap membawa risiko tinggi apabila tidak dilindungi oleh metode pendukung seperti enkripsi dan verifikasi perangkat. Autentikasi berbasis OTP dengan integrasi Firebase merupakan solusi efektif untuk mengurangi risiko akses tidak sah pada aplikasi mobile. Dengan implementasi yang berhasil, sistem ini dapat digunakan sebagai fondasi untuk pengembangan aplikasi yang lebih kompleks dan aman di masa depan.
2. Dengan demonstrasi implementasi ini, kita dapat memahami bagaimana OTP bekerja dalam autentikasi berbasis web. Implementasi ini

INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

juga menunjukkan berbagai kelemahan OTP yang bisa dieksploitasi, seperti intersepsi kode atau phishing. Oleh karena itu, langkah-langkah keamanan tambahan seperti MFA dan enkripsi sangat diperlukan untuk meningkatkan keamanan OTP dalam sistem web.

## VI. Daftar Pustaka

Zhang, Y., Li, J., & Wang, X. (2023). "A Survey on the Security of One-Time Password Authentication Mechanisms in Web Applications." IEEE Access, 11, 87654-87672. DOI: 10.1109/ACCESS.2023.3098765.

Ristenpart, T., Boyen, X., & Shacham, H. (2022). "Security Analysis of OTP-Based Authentication in Web Services: Mitigation of Man-in-the-Middle Attacks." Journal of Computer Security, 30(2), 123-145. DOI: 10.3233/JCS-220006.

Singh, H., & Brown, R. (2021). "Global Adoption and Challenges of OTP in Multi-Factor Authentication Systems." Computers & Security, 103, 102085. DOI: 10.1016/j.cose.2021.102085.

Patel, S., & Sharma, A. K. (2021). "Enhancing Security in Online Banking Using OTP: A Comprehensive Case Study." International Journal of Information Security and Privacy, 15(4), 42-60. DOI: 10.4018/IJISP.2021040103.

Yu, L., & Nielsen, M. (2023). "Future Directions in Multi-Factor Authentication: The Role of OTP and Biometric Integration." IEEE Access, 11, 54321-54335. DOI: 10.1109/ACCESS.2023.3094321.

Kumar, P., & Verma, S. (2022). "Addressing the Security Vulnerabilities of SMS-Based OTP in Financial Transactions." Journal of Information Security and Applications, 63, 102957. DOI: 10.1016/j.jisa.2022.102957.

Gomez, D., & Hernandez, M. (2021). "Mitigating Phishing Attacks on OTP Through Advanced Encryption Techniques." IEEE Transactions on Information Forensics and Security, 16, 3245-3257. DOI: 10.1109/TIFS.2021.3098765.

Rahman, F., & Ahmed, Z. (2022). "Analyzing the Effectiveness of OTP in Cloud-Based Authentication Systems." Journal of Cloud Computing, 9(2), 123-138. DOI: 10.1186/s13677-022-00235-4.

Liu, X., & Wang, Y. (2023). "A Blockchain-Based Solution for Securing OTP in Distributed Web Services." Future Generation Computer Systems, 138, 119-134. DOI: 10.1016/j.future.2023.06.012.

Chen, J., & Zhang, Q. (2021). "Impact of Network Latency on the Security and Usability of OTP in Web Applications." Journal of

INFORMATIKA
Universitas Labuhanbatu
Vol. 12 No. 3, Mei/ 2025
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

Network and Computer Applications, 175, 102924. DOI: 10.1016/j.jnca.2021.102924.

ENISA. (2020). Threat Landscape for Authentication Mechanisms. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu\

Fernandes, E., Rahmati, A., Sugrim, S., Crandall, J., & Prakash, A. (2016). Security Implications of SMS-Based Two-Factor Authentication. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec). DOI: 10.1145/2939918.2939925

Purnomo, A. & Nugroho, R. A. (2023). Pengembangan Aplikasi Mobile Edukasi dengan Kodular dan Firebase untuk Meningkatkan Interaktivitas Pengguna. Jurnal Teknologi dan Sistem Komputer, 11(1), 25–31. https://doi.org/10.14710/jtsiskom.v11i1.25-31

Darmawan, R., Yuliana, N., & Setiawan, B. (2023). Implementasi Firebase Authentication dalam Aplikasi Mobile untuk Sistem Login OTP. Jurnal Teknik Informatika dan Sistem Informasi, 9(2), 112–120. https://doi.org/10.32764/jtisi.v9i2.112120