HMRC Making Tax Digital

API Production Approval Requirements Guide

Comprehensive documentation for software developers seeking production API credentials
and 'HMRC Recognised' software listing status

Version 1.0 | January 2026

This guide consolidates information from official HMRC Developer Hub documentation, UK Government Service Standard, and related compliance frameworks.

Table of Contents

1. Executive Summary

This guide provides comprehensive documentation of the requirements for software developers seeking to obtain production API credentials from HMRC for Making Tax Digital (MTD) services, and to achieve 'HMRC Recognised' software listing status.

Achieving production approval requires fulfilling requirements across multiple domains:

- **Technical compliance** – Successful sandbox testing of all required API endpoints
- **Fraud prevention** – Implementation and validation of mandatory fraud prevention headers
- **Terms of use** – Adherence to HMRC's terms of use and software development practices
- **Accessibility** – WCAG 2.1 Level AA compliance for user-facing software
- **Security** – Appropriate data protection and information security measures
- **Documentation** – Completion of Production Approvals Checklist and supporting evidence

Important: Production access will only be granted after HMRC is satisfied that: (1) the relevant APIs and endpoints have been tested satisfactorily, (2) all required fraud prevention headers are being sent accurately, (3) the software complies with all terms of use, and (4) the Production Approvals Checklist has been completed satisfactorily.

2. Overview of MTD API Approval Process

2.1 What is Making Tax Digital?

Making Tax Digital (MTD) is HMRC's initiative to digitise the UK tax system. It requires businesses to keep digital records and submit tax returns using compatible software that communicates directly with HMRC systems via APIs.

MTD currently covers VAT (mandatory for all VAT-registered businesses since April 2022) and Income Tax Self Assessment (mandatory from April 2026 for income above £50,000, extending to lower thresholds in subsequent years).

2.2 Types of MTD Software

Software Type	Description
End-to-end software	Complete accounting solution that maintains digital records and submits returns directly to HMRC
Bridging software	Links existing digital record-keeping software (e.g., spreadsheets) to HMRC APIs for submission
Combined products	Multiple compatible software products that collectively meet minimum functionality standards

2.3 Production Approval Pathway

The pathway to production credentials follows these key stages:

1. **Register on HMRC Developer Hub** – Create an account and register your application
2. **Review API Documentation** – Understand required endpoints and integration patterns
3. **Develop Software** – Build your application following HMRC guidelines
4. **Create Sandbox Application** – Register for sandbox testing credentials
5. **Test in Sandbox** – Thoroughly test all required API endpoints
6. **Validate Fraud Headers** – Ensure fraud prevention headers pass validation
7. **Request Production Credentials** – Apply for production access
8. **Complete Production Approvals Checklist** – Provide required documentation
9. **HMRC Review** – HMRC reviews testing evidence and checklist
10. **Production Access Granted** – Receive production credentials and API access

3. Prerequisites for Production Access

3.1 Developer Hub Registration

Before beginning development, you must register on the HMRC Developer Hub at developer.service.hmrc.gov.uk. Registration allows you to:

- Create and manage sandbox and production applications
- Subscribe to required APIs
- Access API documentation and testing tools
- Receive important updates about API changes
- Submit requests for production credentials

Application Naming: Your production application name should match your organisation name. You only need one Developer Hub production application regardless of how many APIs you use.

3.2 Sandbox Testing Requirements

HMRC requires comprehensive testing in the sandbox environment before production access is granted. Testing requirements include:

- Test all API endpoints that your software will use in production
- Use the Create Test User API to generate test credentials (test VRN, User ID, Password)
- Test fraud prevention headers using the Test Fraud Prevention Headers API
- Document the dummy National Insurance Number used in sandbox testing
- Contact SDSTeam@hmrc.gov.uk within 14 days of completing testing to allow HMRC to view logs
- Test different scenarios using Gov-Test-Scenario headers where available

3.3 Required API Endpoints (VAT MTD)

For VAT (MTD), the following endpoints are mandatory for production approval:

Endpoint	Purpose	Required
Retrieve VAT obligations	Get obligation periods for VAT returns	Yes
Submit VAT return for period	Submit the VAT return data	Yes
View VAT return	Retrieve previously submitted returns	Recommended
Retrieve VAT customer information	Check registration details and Flat Rate status	Recommended
Retrieve VAT liabilities	Get outstanding VAT liabilities	Optional
Retrieve VAT payments	Get payment history	Optional
Retrieve VAT penalties	Get penalty information	Optional

4. Terms of Use Compliance

Compliance with HMRC's Terms of Use is mandatory for production access. The terms establish expectations for both software developers and HMRC.

4.1 Core Terms of Use

When applying for production access, you will be asked to confirm compliance with terms covering:

- **Data Protection** – Compliance with UK GDPR and Data Protection Act 2018
- **Customer Data Security** – Appropriate measures to protect customer data
- **Customer Ownership** – End users must own and have access to all their records
- **Data Portability** – Users must be able to export their records if necessary
- **Fraud Prevention** – Submission of required fraud prevention header data
- **Accurate Information** – Not misleading customers about software capabilities
- **Support Obligations** – Maintaining and supporting your solution adequately

4.2 What HMRC Expects from Developers

- Provide compliant fraud prevention header information for all MTD APIs
- Ensure customers have a streamlined end-to-end journey
- Support everything a business customer needs to meet their tax obligations
- Safeguard customer data and protect HMRC systems against fraud
- Maintain software to enable clients to meet their MTD obligations
- Not use customer information for purposes beyond fulfilling MTD obligations without consent
- Respond to security incidents promptly and notify HMRC where appropriate

4.3 What Developers Can Expect from HMRC

- 6 months notice before breaking changes are made in production
- Breaking changes published to sandbox environment first where possible
- Response to support queries within 2 working days
- Regular updates on API changes and deprecations
- Access to comprehensive API documentation
- Sandbox environment for testing

4.4 Consequences of Non-Compliance

If your software fails to meet HMRC's terms of use, access to APIs may be removed temporarily or permanently. Situations that may result in access removal include:

- Using customer information for purposes not consented to
- Serious data or cybersecurity concerns
- Repeated failure to maintain and support your solution
- Breach of tax or social security payment obligations

- Violating the terms of use or spirit of collaboration

HMRC maintains a software developer register on GOV.UK and may remove listings for developers who do not behave in accordance with the spirit of the terms of collaboration.

5. Fraud Prevention Headers

5.1 Legal Requirements

> **Warning: You are required by law to submit fraud prevention header data for the VAT (MTD) and Income Tax Self Assessment (MTD) APIs. This includes all associated APIs and endpoints. This requirement must be fulfilled before Production access can be granted.**

HMRC uses fraud prevention header data to:

- Support prosecutions for tax and duty fraud
- Monitor and audit transactions
- Protect taxpayers' data from fraudulent activities
- Maintain security of HMRC systems

5.2 Required Headers by Connection Method

The specific headers required depend on your software's connection method. Common connection methods and their requirements include:

WEB_APP_VIA_SERVER (Web application via server):

- Gov-Client-Connection-Method
- Gov-Client-Browser-JS-User-Agent
- Gov-Client-Browser-Plugins
- Gov-Client-Device-ID
- Gov-Client-Local-IPs
- Gov-Client-Public-IP
- Gov-Client-Screens
- Gov-Client-Timezone
- Gov-Client-User-Agent
- Gov-Client-Window-Size
- Gov-Vendor-Product-Name
- Gov-Vendor-Public-IP
- Gov-Vendor-Version

BATCH_PROCESS_DIRECT (Batch processing):

- Gov-Client-Connection-Method
- Gov-Vendor-Product-Name
- Gov-Vendor-Version
- Gov-Vendor-Public-IP

5.3 Testing Fraud Prevention Headers

Use the Test Fraud Prevention Headers API to validate your header implementation:

1. **Initial Development** – Use the /validate endpoint for immediate feedback on single requests

2. **Integration Testing** – Run tests in sandbox with headers enabled
3. **Validation Feedback** – Use /validation-feedback endpoint to check last request to each endpoint
4. **Fix All Errors** – Resolve all errors identified by the validation API
5. **Address Advisories** – Review and address any warnings/advisories

HMRC uses your most recent submissions to the sandbox to check fraud prevention headers. Do not send HMRC your logs from the Test Fraud Prevention Headers API.

6. Technical Requirements

6.1 Security Standards

• **TLS 1.2 or higher** – All HMRC APIs are only accessible over TLS (HTTPS). Applications must support TLS 1.2 or higher.

• **Certificate Management** – Do not pin HMRC-specific certificates. Use a global root CA keystore as certificates may change.

• **IP Allow List** – Optional security feature for static IP addresses. Configure in Developer Hub if applicable.

• **Secure Storage** – OAuth tokens and sensitive data must be stored securely.

• **Network Configuration** – Configure proxy (not firewall) for HMRC domain access.

6.2 OAuth 2.0 Implementation

HMRC uses OAuth 2.0 for user-restricted endpoints. Key requirements:

• Implement OAuth 2.0 authorization code flow for user authentication

• Handle refresh tokens appropriately (authorization codes valid for 10 minutes only)

• Define correct scopes for each API (e.g., read:vat, write:vat)

• Specify valid redirect URIs when creating applications

• Do not automate driving of OAuth web interfaces

• Handle token expiration and refresh gracefully

6.3 Error Handling

Build robust error handling for HMRC API responses:

HTTP Code	Category	Action
200-299	Success	Process response normally
400-499	Client Error	Fix request or inform user of issue
429	Too Many Requests	Back off temporarily, then retry
500-599	Server Error	Retry with exponential backoff

6.4 API Rate Limits

HMRC applies rate limits to encourage real-time interactions and protect backend services:

• Standard limit: 3 requests per second per application

• Some APIs (e.g., CDS) may have different pre-approved limits

• Avoid batching requests – rate limits encourage real-time calls

• If receiving 429 responses regularly, contact HMRC to discuss application design

• Implement appropriate backoff strategies for 429 responses

7. Accessibility Requirements (WCAG 2.1 AA)

Software with user-facing interfaces must meet Web Content Accessibility Guidelines (WCAG) 2.1 Level AA standards. This is assessed through HMRC's WCAG 2.1 AA Questionnaire as part of the production approval process.

7.1 WCAG 2.1 Overview

WCAG 2.1 is organized around four principles (POUR):

- **Perceivable** – Information must be presentable in ways users can perceive
- **Operable** – Interface components must be operable by all users
- **Understandable** – Information and operation must be understandable
- **Robust** – Content must be robust enough for assistive technologies

7.2 Key Requirements

- Provide text alternatives for non-text content
- Ensure content is accessible via keyboard alone
- Provide sufficient colour contrast (minimum 4.5:1 for normal text)
- Make text resizable up to 200% without loss of functionality
- Ensure forms have clear labels and error identification
- Provide consistent navigation and predictable behavior
- Support screen readers and other assistive technologies

7.3 Testing Tools

Recommended tools for accessibility testing include:

- Pa11y – Automated accessibility testing tool
- axe-core – Accessibility testing engine
- WAVE – Web accessibility evaluation tool
- Manual keyboard testing
- Screen reader testing (NVDA, JAWS, VoiceOver)

8. UK Government Service Standard

While primarily aimed at government services, the UK Government Service Standard provides useful guidance for software developers building MTD-compatible applications. HMRC expects software to align with these principles where applicable.

The 14 Points of the Service Standard:

1. **Understand users and their needs**: Research to understand who uses the service and what they need
2. **Solve a whole problem for users**: Work to solve the complete problem, not just part of it
3. **Provide a joined up experience**: Work with other channels to provide a coherent experience
4. **Make the service simple to use**: Build something simple and intuitive
5. **Make sure everyone can use the service**: Ensure the service is accessible to all users
6. **Have a multidisciplinary team**: Put together the right team for the job
7. **Use agile ways of working**: Build incrementally and iterate based on feedback
8. **Iterate and improve frequently**: Keep improving the service based on user feedback
9. **Create a secure service**: Protect users' privacy and evaluate security risks
10. **Define success and publish data**: Understand what good looks like and publish performance data
11. **Choose the right tools and technology**: Select technology that allows flexibility
12. **Make new source code open**: Make source code open where possible
13. **Use open standards and patterns**: Build on open standards and common patterns
14. **Operate a reliable service**: Minimize downtime and have a support plan

9. Data Protection & Security

9.1 ICO Information Security Requirements

Software handling personal data must comply with UK GDPR and implement appropriate security measures. Key requirements from ICO guidance include:

- **Risk Assessment** – Identify, assess and manage information security risks
- **Security Policy** – Have an approved information security policy that is regularly reviewed
- **Defined Responsibilities** – Allocate clear information security responsibilities
- **Third-Party Agreements** – Written contracts with processors ensuring data protection
- **Data Protection by Design** – Conduct DPIAs for high-risk processing
- **Incident Response** – Have procedures for identifying and responding to breaches

9.2 NCSC Penetration Testing Guidance

The National Cyber Security Centre (NCSC) provides guidance on penetration testing. While not mandatory for all MTD software, regular security testing is strongly recommended:

- Consider regular vulnerability assessments and penetration testing
- Use CHECK-certified providers for government/CNI work
- CREST-accredited testers provide international standard assurance
- Test both infrastructure and application security
- Address identified vulnerabilities promptly
- Document testing and remediation activities

For services handling sensitive government data, CHECK-certified penetration testing may be required. CHECK is the NCSC's scheme for approving companies to conduct authorized penetration tests on public sector systems.

10. Production Approvals Checklist

HMRC will issue a Production Approvals Checklist asking for details about your software. This must be completed and returned to the Software Developer Support Team (SDSTeam@hmrc.gov.uk). Production access will be granted after HMRC is satisfied with your submission.

10.1 Information Required

The checklist typically requests the following information:

- Company details (name, registration number, contact information)
- Software product name and description
- Target user base (businesses, agents, specific sectors)
- Product type (end-to-end, bridging, filing-only, etc.)
- VAT schemes supported (if applicable)
- API endpoints implemented and tested
- Sandbox testing credentials used
- Fraud prevention header implementation details
- Accessibility compliance evidence
- Privacy policy and terms of service URLs
- Support arrangements for customers

10.2 Evidence Requirements

- **Testing Evidence** – Sandbox credentials and test data for HMRC to verify API calls
- **Fraud Header Validation** – Evidence of successful fraud prevention header validation
- **Accessibility Report** – WCAG 2.1 AA compliance assessment results
- **Privacy Documentation** – Links to published privacy policy
- **Test Report** – Documentation of testing conducted

Important: Contact SDSTeam@hmrc.gov.uk within 14 days of completing your API testing. This enables HMRC to view the testing data within their logs before it is purged.

11. Software Choices Listing

HMRC publishes a list of compatible software (Software Choices) on GOV.UK. Being listed as 'HMRC Recognised' software provides visibility to potential customers seeking MTD-compatible solutions.

11.1 Listing Requirements

- Completed production approval process successfully
- All required APIs tested and functioning correctly
- Fraud prevention headers validated and accurate
- WCAG 2.1 AA compliance demonstrated
- Terms of use accepted and adhered to
- Product actively supported and maintained

11.2 Request Listing

Software providers may request to be added to the Software Choices list when they have completed the necessary steps in the Production Approvals process. Contact the Software Developer Support Team to request listing.

11.3 Free Software Requirements

If providing free software, additional requirements apply:

- Enable customers to meet MTD obligations for a full accounting period at no cost
- Include free digital record keeping where applicable
- Support required submission types without charge
- No requirement to include VAT, Corporation Tax, or PAYE functionality
- No requirement to link with agent products

12. Ongoing Compliance

Production approval is not a one-time event. Ongoing compliance requires continuous attention to:

12.1 API Updates and Versioning

- Monitor HMRC announcements for API changes and deprecations
- Subscribe to API version updates in Developer Hub
- Test new API versions in sandbox before they reach production
- Plan for migration when API versions are deprecated (typically 6+ months notice)
- Run automated tests weekly against sandbox to catch changes early

12.2 Breaking Changes

HMRC defines breaking changes as changes requiring software modifications. These include:

- Removing an endpoint or HTTP method
- Adding mandatory request fields
- Changing field types or formats
- Removing response fields
- Changing URL structures
- Modifying authentication requirements

12.3 Ongoing Testing Requirements

- For access to updated APIs, evidence of satisfactory testing is required
- New Production Approvals Checklist not generally required for version updates
- Continue validating fraud prevention headers with each release
- Maintain accessibility compliance through regular testing
- Address any issues identified by HMRC promptly

13. Key Contacts and Resources

13.1 HMRC Contacts

Contact	Email/URL
Software Developer Support Team	SDSTeam@hmrc.gov.uk
Developer Hub	developer.service.hmrc.gov.uk
Production Credentials Requests	Via Developer Hub portal

13.2 Key Documentation URLs

HMRC Developer Hub

https://developer.service.hmrc.gov.uk/api-documentation

VAT MTD End-to-End Guide

https://developer.service.hmrc.gov.uk/guides/vat-mtd-end-to-end-service-guide/

VAT API Documentation

https://developer.service.hmrc.gov.uk/api-documentation/docs/api/service/vat-api/1.0

Terms of Use

https://developer.service.hmrc.gov.uk/api-documentation/docs/terms-of-use

Development Practices

https://developer.service.hmrc.gov.uk/api-documentation/docs/development-practices

Fraud Prevention

https://developer.service.hmrc.gov.uk/guides/fraud-prevention/

Reference Guide

https://developer.service.hmrc.gov.uk/api-documentation/docs/reference-guide

UK Service Standard

https://www.gov.uk/service-manual/service-standard

WCAG 2.1 Guidelines

https://www.w3.org/WAI/standards-guidelines/wcag/

ICO Security Guidance

https://ico.org.uk/for-organisations/

NCSC Pen Testing

https://www.ncsc.gov.uk/guidance/penetration-testing

13.3 Support Response Times

HMRC aims to respond to queries not resolved at point of contact within 2 working days, with further updates every 2 working days if required.

Quick Reference Checklist

Use this checklist to track progress toward production approval:

- ■ Registered on HMRC Developer Hub
- ■ Reviewed API documentation and service guides
- ■ Created sandbox application
- ■ Subscribed to required APIs
- ■ Implemented OAuth 2.0 authentication
- ■ Implemented all required API endpoints
- ■ Implemented fraud prevention headers
- ■ Tested all endpoints in sandbox
- ■ Validated fraud prevention headers using test API
- ■ Resolved all fraud header errors and advisories
- ■ Completed accessibility testing (WCAG 2.1 AA)
- ■ Implemented appropriate error handling
- ■ Published privacy policy
- ■ Contacted HMRC within 14 days of completing testing
- ■ Created production application in Developer Hub
- ■ Completed Production Approvals Checklist
- ■ Submitted checklist to SDSTeam@hmrc.gov.uk
- ■ Received production credentials
- ■ Requested Software Choices listing (optional)

This guide is provided for informational purposes and consolidates publicly available HMRC documentation. Always refer to official HMRC sources for the most current requirements. Contact SDSTeam@hmrc.gov.uk for clarification on specific requirements.